PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

PERFIL DEL TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MASTER EN REDES DE COMUNICACION

TEMA

"ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE CALIDAD DE SERVICO (QoS) EN LA RED LAN Y WAN DE LA UNIDAD DE NEGOCIOS CELEC TERMOPICHINCHA"

JUAN PABLO LOPEZ FIERRO

QUITO - 2016

DEDICATORIA

A mi familia que siempre estará presente en toda mi vida, apoyándome, respaldándome y dándome el aliento para finalizar con las metas y objetivos planteados a nivel profesional y personal.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

INTRODUCCIÓN

1.1 Antecedentes

La Unidad de Negocios Termopichincha contribuye al bienestar y desarrollo nacional, mediante la producción de energía eléctrica con altos índices de disponibilidad, confiabilidad y eficiencia, con su talento humano comprometido y competente, actuando responsablemente con la comunidad y el ambiente, fortalecido con una infraestructura extensa y solida, soportando todos los servicios internos y externos necesarios para el cumplimiento de las funciones de cada persona que conforma la Unidad de Negocios.

La Unidad de Negocios Termopichincha se apoya en el mejoramiento continuo como actividad estratégica dentro del plan operativo anual del departamento de tecnología y de la organización. La creación de nuevos proyectos internos que benefician a las diferentes áreas vienen acompañados con el cambio de la tecnología y los beneficios que esta brinda.

Crear una solución de comunicaciones para redes convergentes permitirá a las organizaciones conseguir mayor seguridad, resistencia, flexibilidad y escalabilidad, dotando de servicios consistentes a todos los funcionarios de la organización, por ello desde el punto de vista de la transmisión y recepción de la información es importante que la infraestructura de red pueda superar los problemas más frecuentes como retardos, latencia, pérdida de paquetes, baja de rendimiento, jitter y ancho de banda que afectan al flujo de datos y especialmente a los datos de VoIP, al implementar mecanismos de QoS se puede superar dichos inconvenientes y se puede controlar el comportamiento de la red con la utilización de dispositivos apropiados.

La Unidad de Negocios Termopichincha fue una organización privada conformada por 50 personas aproximadamente, los cuales manejaban pocos servicios informáticos internamente. Cuando Termopichincha comenzó a crecer, tanto en recurso humano como en infraestructura tecnológica, los servicios internos al igual que los requerimientos se incrementaron.

Actualmente la Unidad de Negocios Termopichincha está conformada por 400 personas aproximadamente, las cuales se encuentran distribuidas en diferentes regiones del país y hacen uso de más de 25 servicios de red como VoIP, sistemas financieros, correo electrónico, datos industriales, etc.

Este proyecto presentará un estudio y definición de los conceptos relacionados con calidad de servicio (QoS). Luego se realizará un análisis e identificación del tráfico en la red de la Unidad de Negocios Termopichincha, utilizando los procedimientos de calidad de servicio (QoS) se definirán los mecanismos más adecuados de calidad del servicio para el tráfico de red y finalmente se implementará el mecanismo de calidad de servicio en la infraestructura de red LAN y WAN logrando que la infraestructura de red cumpla con el nivel óptimo de rendimiento para el flujo de datos y la habilidad necesaria para priorizar los diferentes servicios.

Debido al crecimiento y avance tecnológico en el mundo de Internet, los sistemas informáticos ya no solo se basan en una red de datos, sino que ahora también se hace uso de voz y video. El auge de la telefonía IP es algo evidente y la principal razón es el reaprovechamiento de los recursos y la disminución en el costo de llamadas a través de Internet. Sin embargo, si de algo adolece todavía la VoIP es de la calidad de los sistemas telefónicos tradicionales. Los problemas de esta calidad son muchas veces inherentes a la utilización de la red (Internet y su velocidad y ancho de banda) y podrán irse solventando, por lo que es necesaria la

implementación de QoS, cuya tarea primordial es asegurar determinadas características como la calidad y confiabilidad en la transmisión de la información evitando el congestionamiento de la red. (Elastixtech, 2016)

En el ámbito mundial, existe la tendencia a usar redes conmutadas (conmutación de paquetes, tramas y celdas) para servicios del tipo ancho de banda bajo demanda. El protocolo de Internet (IP), que ha sido utilizado en estas redes durante las tres últimas décadas para el intercambio de información entre los diferentes ordenadores, ha terminado imponiéndose como el protocolo más usado. A la fecha nuevas aplicaciones han surgido, creando el desafío de cómo adaptar la Internet a estos nuevos cambios y necesidades. Hoy en estas redes se caracterizan por manejar distintos tipos de tráfico de una manera eficiente. Esto les es posible lograrlo, ya que las redes, manejan el concepto de "Calidad del Servicio (QoS)", la cual se define en términos de parámetros relacionados con las pérdidas y retardos en la transferencia de celdas. (Oocities, 2016) (Ataucuri, 1999)

Aumentar el tráfico en una red, se hace cada vez más importante para los departamentos de TI equilibrar el rendimiento de la red con el costo de servicio. Sin embargo, el tráfico de red no es fácil de priorizar y administrar. Aplicaciones de misión crítica y sensible a la latencia deben competir por el ancho de banda contra el tráfico de menor prioridad. Al mismo tiempo, algunos usuarios y equipos con el rendimiento de la red específica podrían necesitar diferenciar los niveles de servicio. Estos retos de proporcionar niveles de rendimiento de red rentable y predecible a menudo aparecen en conexiones de red (WAN) de área amplia o con aplicaciones sensibles a la latencia, como voz sobre IP (VoIP) y video. Sin embargo, el objetivo final de proporcionar los niveles de servicio de red predecible se aplica a cualquier entorno de red y a

más de las aplicaciones de VoIP, a las aplicaciones personalizadas de línea de negocio de su empresa. (Microsoft, 2016)

Fundamentalmente, QoS le permite brindar un mejor servicio a ciertos flujos. Esto se hace para elevar la prioridad de un flujo o limitar la prioridad de otro flujo. Cuando se utilizan herramientas de administración de congestión, se intenta aumentar la prioridad de un flujo en cola y mantener colas de diferentes maneras. Enviar flujos de mayor prioridad antes de los flujos de menor prioridad. (Lin, 1999) (Cisco, 1999)

La calidad de servicios comprende requerimientos en todos los aspectos de una conexión, tales como tiempo de respuesta de los servicios, pérdidas, relación señal ruido, diafonías, eco, interrupciones, frecuencia de respuesta, niveles de sonido, entre otros. Una sub categoría de calidad de servicios de telefonía son los requerimientos de nivel de servicio, los cuales comprenden aspectos de una conexión relacionados con la capacidad y cobertura de una red, por ejemplo garantizar la probabilidad máxima de bloqueo y la probabilidad de interrupción. (Wikipedia)

1.2 Justificación

La infraestructura tecnológica actual de la Unidad de Negocios Termopichincha soporta a más de 25 servicios internos que son consumidos por todos los usuarios pero no existen los mecanismos apropiados para controlar el comportamiento de la red para que esta provea un servicio eficiente a los usuarios y a las aplicaciones requeridas.

El consumo de los servicios no es manejado adecuadamente por los usuarios provocando que el uso excesivo de uno afecte el desempeño de otros, pues, servicios de menor prioridad afectan a los servicios de mayor prioridad. Con la implementación de calidad de servicios la infraestructura del negocio tendrá la capacidad de garantizar y de controlar una asignación de recursos adecuada y una diferenciación del servicio conforme a las aplicaciones solicitadas.

La necesidad de superar los retos que presenta la red de la Unidad de Negocios Termopichincha como control de ancho de banda, retardo, jitter y pérdida de paquetes permitirán que los servicios internos sean más eficientes y brinden la mejor respuesta a los usuarios según sus requerimientos.

La comunicación interna de la Unidad de Negocio Termopichincha es afectada directamente por la saturación innecesaria de tráfico dentro de la infraestructura de red y el desperdicio de recursos como el ancho de banda.

La comunicación basada en telefonía IP es uno de los servicios más importantes requeridos dentro de la Unidad de Negocios Termopichincha pues maneja tráfico más sensible y requiere de tratamiento especial para priorizarlo y brindar la mejor respuesta. El proyecto pretende colocar el modelo de QoS para mejorar este servicio y mantener siempre una comunicación constante y

continua entre los departamentos, oficinas, centrales y sitios remotos, como también, mejorar los servicios de videoconferencia.

Dentro de la Unidad de Negocios Termopichincha se maneja un equipamiento de comunicaciones CISCO actualizado cuya capacidad es subutilizada. Este proyecto pretender sacar provecho del equipamiento de comunicaciones y aprovechar los beneficios que conlleva la implementación de un modelo de calidad de servicio, tanto en su parte LAN como en su parte WAN.

La implementación de un modelo de QoS pretende acelerar los procesos internos financieros mejorando la comunicación con el sistema financiero de la corporación, como también, mejorar los procesos de los diferentes departamentos en los cuales se manejan otras aplicaciones que requieren de un tratamiento especial de la información dentro de la red.

La Unidad de Negocios Termopichincha pretende que sus empleados utilicen los recursos de red de la mejor manera pensando siempre en el beneficio de la corporación. La infraestructura de red LAN y WAN debe estar preparada para brindar los mejores recursos y servicios internos permitiendo a sus empleados la utilización eficiente, rápida y continua de la información.

Este proyecto permitirá dar la prioridad más alta al tráfico más crítico que se maneja dentro de la Unidad de Negocios Termopichincha y que no puede sufrir inconvenientes durante su transmisión y recepción, como por ejemplo, los datos de generación de energía de las centrales en tiempo real, comunicación de voz, videoconferencia, aplicativos financieros, correo electrónico, aplicativos de colaboración y los demás tipos de tráfico de datos que se maneja dentro de la red.

1.3 Objetivos

1.3.1 Objetivo General

Analizar la infraestructura LAN - WAN de la Unidad de Negocios Termopichincha con el fin de diseñar e implementar un modelo de calidad de servicio (QoS) que permita asegurar un nivel de servicio adecuado para cada clase de tráfico dentro de la Unidad de Negocios Termopichincha.

1.3.2 Objetivos Específicos

- Estudiar y definir los conceptos relacionados con calidad de servicio (QoS).
- Analizar e identificar el tráfico de red de la Unidad de Negocios utilizando los procedimientos de calidad de servicio (QoS).
- Definir el modelo de calidad de servicio más adecuado para el tráfico de red de la Unidad de Negocios Termopichincha.
- Implementar el modelo de calidad de servicio en la infraestructura de red LAN y WAN de la Unidad de Negocios Termopichincha.

1.4 Alcance

La implementación del modelo de calidad de servicio en la infraestructura de red de la Unidad de Negocios Termopichincha enfocada en los siguientes puntos:

- Implementación de calidad de servicio en la parte LAN, que comprende 9 sitios que mantienen equipos de comunicación independientes, los cuales forman una topología en estrella, centralizando en un switch de Core principal.
- Implementación de calidad de servicio en la parte WAN, que comprende 4 enlaces de datos hasta llegar al equipo perimetral de la Unidad de Negocios Termopichincha.

1.5 Factibilidad

1.5.1 Factibilidad Técnica

La Unidad de Negocios Termopichincha cuenta con una red convergente la cual soporta diferentes tipos de aplicaciones simultáneamente sobre una misma infraestructura enfrentando los diferentes restos como ancho de banda, retardo, jitter y perdida de paquetes, por lo que técnicamente es factible implementar un modelo de calidad de servicio QoS para superar estos retos.

Adicionalmente es técnicamente factible ya que el equipamiento de comunicaciones actual permite la configuración e implementación de este tipo de solución.

1.5.2 Factibilidad Económica

La Unidad de Negocios Termopichincha cuenta con todo el equipamiento de comunicaciones en su infraestructura LAN y WAN necesario para la ejecución del proyecto, por lo tanto no requiere la compra de equipamiento adicional.

1.5.3 Factibilidad Operativa

Para el análisis, diseño e implementación de calidad de servicio QoS en la red lan y wan contaremos con el apoyo de la Unidad de Negocios Termopichincha, la cual autoriza el acceso a los recursos, equipamiento e información que se necesiten para el desarrollo de este proyecto.

1.6 Hipótesis

Si se implementa un modelo de calidad de servicio (QoS), entonces se brindarán alternativas que permitan asegurar un nivel de servicio adecuado para cada clase de tráfico dentro de la Unidad de Negocios Termopichincha.

Identificación de variables:

Variable independiente: Modelo de calidad de servicio (QoS).

Variable dependiente: Tráfico de red, identificación del tráfico, requerimientos del negocio, políticas

CAPÍTULO 2

MARCO TEÓRICO

2.1 Calidad de Servicio QoS

2.1.1 Introducción a la QoS

Debido al crecimiento y avance tecnológico en el mundo de Internet, los sistemas informáticos ya no solo se basan en una red de datos, sino que ahora también se hace uso de voz y video. El auge de la telefonía IP es algo evidente y la principal razón es el reaprovechamiento de los recursos y la disminución en el costo de llamadas a través de Internet. Sin embargo, si de algo adolece todavía la VoIP es de la calidad de los sistemas telefónicos tradicionales. Los problemas de esta calidad son muchas veces inherentes a la utilización de la red (Internet y su velocidad y ancho de banda) y podrán irse solventando, por lo que es necesaria la implementación de QoS, cuya tarea primordial es asegurar determinadas características como la calidad y confiabilidad en la transmisión de la información evitando el congestionamiento de la red. (Elastixtech, 2016)

En el ámbito mundial, existe la tendencia a usar redes conmutadas (conmutación de paquetes, tramas y celdas) para servicios del tipo ancho de banda bajo demanda. El protocolo de Internet (IP), que ha sido utilizado en estas redes durante las tres últimas décadas para el intercambio de información entre los diferentes ordenadores, ha terminado imponiéndose como el protocolo más usado. A la fecha nuevas aplicaciones han surgido, creando el desafío de cómo adaptar la Internet a estos nuevos cambios y necesidades. Hoy en estas redes se caracterizan por manejar distintos tipos de tráfico de una manera eficiente. Esto es posible lograrlo, ya que las redes,

manejan el concepto de “Calidad del Servicio (QoS)”, la cual se define en términos de parámetros relacionados con las pérdidas y retardos en la transferencia de celdas. (Oocities, 2016) (Ataucuri, 1999)

Aumenta el tráfico en una red, se hace cada vez más importante para los departamentos de TI equilibrar el rendimiento de la red con el costo de servicio. Sin embargo, el tráfico de red no es fácil de priorizar y administrar. Aplicaciones de misión crítica y sensible a la latencia deben competir por el ancho de banda contra el tráfico de menor prioridad. Al mismo tiempo, algunos usuarios y equipos con el rendimiento de la red específica podrían requerir requisitos que diferencian los niveles de servicio. Estos retos de proporcionar niveles de rendimiento de red rentable y predecible a menudo aparecen en conexiones de red (WAN) de área amplia o con aplicaciones sensibles a la latencia, como voz sobre IP (VoIP) y video. Sin embargo, el objetivo final de proporcionar los niveles de servicio de red predecible se aplica a cualquier entorno de red y a más de las aplicaciones de VoIP, a las aplicaciones personalizadas de línea de negocio de su empresa. (Microsoft, 2016)

Fundamentalmente, QoS le permite brindar un mejor servicio a ciertos flujos. Esto se hace para elevar la prioridad de un flujo o limitar la prioridad de otro flujo. Cuando se utilizan herramientas de administración de congestión, se intenta aumentar la prioridad de un flujo en cola y mantener colas de diferentes maneras. Enviar flujos de mayor prioridad antes de los flujos de menor prioridad. (Lin, 1999) (Cisco, 1999)

La calidad de servicios comprende requerimientos en todos los aspectos de una conexión, tales como tiempo de respuesta de los servicios, pérdidas, ratio señal a ruido, diafonías, eco, interrupciones, frecuencia de respuesta, niveles de sonido, entre otros. Una sub categoría de

calidad de servicios de telefonía son los requerimientos de nivel de servicio, los cuales comprenden aspectos de una conexión relacionados con la capacidad y cobertura de una red, por ejemplo garantizar la probabilidad máxima de bloqueo y la probabilidad de interrupción. (Wikipedia)

2.1.2 Parámetros de QoS

Como se indicó anteriormente, los mayores retos que presenta una red convergente y que están relacionados directamente con la mejora de la calidad de servicio son:

2.1.2.1 Ancho de Banda

En conexiones a Internet el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (bps), kilobites por segundo (kbps), o megabites por segundo (mps). En las redes de ordenadores, el ancho de banda a menudo se utiliza como sinónimo para la tasa de transferencia de datos, la cantidad de datos que se puedan llevar de un punto a otro en un período dado (generalmente un segundo). Esta clase de ancho de banda se expresa generalmente en bites por segundo (bps). (Masadelante, 1999 - 2016)

La falta de ancho de banda puede impactar en los flujos de trabajo de las aplicaciones que corren y compiten por un porcentaje de ancho de banda sobre una conexión desde un sitio a otro, provocando que se presenten inconvenientes de pérdida de paquetes, retardos de entrega y recepción, etc. El aumento del ancho de banda en un canal de datos podría evitar estos inconvenientes, pero el costo podría ser un limitante, por ello se debe aplicar otro tipo de métodos que permitan que los flujos de trabajo manejen un determinado ancho de banda.

2.1.2.2 End-To-End Delay

El Delay o Retraso es el tiempo que se demoran en llegar los paquetes desde su origen hasta su destino. Este retraso se puede presentar por diferentes motivos, entre los más importantes:

- *Procesamiento*: El tiempo de procesamiento de los paquetes provocados por los equipo de red (router o switch). Tiempo en que el paquete ingresa hasta que es colocado en la cola de salida.
- *Encolamiento*: El tiempo en que el paquete permanece en las colas de salida de los equipos de red (router o switch). El performance del equipo de red juega un papel muy importante en cuanto al encolamiento (velocidad y ancho de banda de la interface).
- *Propagación*: El tiempo tomado por el paquete en atravesar por todo el medio para llegar a su destino. El medio puede ser fibra óptica, cobre, radios, etc.

2.1.2.3 Variación de Retardo (Jitter)

A partir de la definición del delay, el Jitter es la variación de tiempo de retraso entre los diferentes paquetes de un mismo flujo. En el caso de la transmisión de datos relacionados con voz y video, la variación de tiempo provoca que se presenten inconvenientes de distorsión, voz entrecortada y retardo de tiempo real, por ello, es muy importante que los paquetes lleguen a su destino con la misma velocidad y orden que fueron enviados desde el origen.

Existen valores definidos para los diferentes tipos de datos en cuanto a estos parámetros, los cuales, deben ser fijados dentro de una red para brindar el mejor servicio.

La solución más ampliamente adoptada es la utilización del jitter buffer. El jitter buffer consiste básicamente en asignar una pequeña cola o almacén para ir recibiendo los paquetes y sirviéndolos con un pequeño retraso. Si algún paquete no está en el buffer (se perdió o no ha llegado todavía) cuando sea necesario se descarta. Normalmente en los teléfonos IP (hardware y software) se pueden modificar los buffers. Un aumento del buffer implica menos perdida de paquetes pero más retraso. Una disminución implica menos retardo pero más pérdida de paquetes. (Elastixtech, 2016)

2.1.2.4 Pérdida de Paquetes (Packet Loss)

La perdida de paquetes se presenta tanto en los equipos de comunicación, debido a la congestión en sus interfaces, como también, durante la transmisión. El tipo de tráfico TCP/IP tiene la característica de volver a retransmitir los paquetes, pero el tráfico UDP, no posee esta característica.

En el caso de los equipos de comunicación la perdida de paquetes se presenta debido a problemas de congestión, ancho de banda de las interfaces y tamaño en los buffers.

2.1.3 Modelos de QoS

Existen 3 modelos de calidad de servicios para ser aplicados dentro de las redes de datos:

2.1.3.1 Modelo Best-Effort

Gerometta (2010) indica que el modelo Best-Effort es el modelo aplicado en Internet, y el que aplica por defecto toda red que no tiene políticas explícitamente definidas. No garantiza

ningún tratamiento o recurso específico a ningún flujo de información. Todo paquete es tratado de igual forma, no hay tratamiento preferencial.

Las principales características del modelo son:

- Altamente escalable.
- No requiere mecanismos o configuraciones especiales.
- No garantiza recursos ni diferencia ningún tipo de servicio.

2.1.3.2 Modelo IntServ

Gerometta (2010) indica que el modelo IntServ es un modelo de implementación de servicio bajo demanda. Tiene como objetivo garantizar recursos disponibles a lo largo de una ruta para una aplicación específica. Antes de iniciarse propiamente la sesión de la aplicación se señaliza la ruta para verificar la disponibilidad de los recursos necesarios para un adecuado desarrollo de la misma.

Una vez que la aplicación realiza la reserva de recursos la misma se mantiene aún cuando la aplicación no la esté utilizando, hasta tanto se levante la reserva de recursos. Permite garantizar las condiciones de operación de aplicaciones críticas. (Gerometta, 2010)

Sus características más importantes son:

- Negocia condiciones específicas de calidad de servicio antes de que se inicie la comunicación propiamente dicha.
- Una vez hecha la reserva, la aplicación cuenta con los recursos reservados más allá de la situación de tráfico de la red.

- Puede adecuarse a demandas específicas y diferentes de cada tipo de tráfico o aplicación.
- La reserva de recursos se realiza para cada flujo de información en particular. No se reservan recursos en función de la aplicación genéricamente.
- Cuando se asocia a desarrollos de telefonía IP, da una aproximación orientada a la conexión para este tipo de servicios. Cada dispositivo a lo largo de la ruta configura y mantiene la operación de cada comunicación individualmente.
- Utiliza los servicios de RSVP (Resource Reservation Protocol).
- No es escalable en grandes redes o implementaciones muy complejas.

2.1.3.2.1 RSVP

Ataucuri (1999) indica que Resourse Reservation Protocol es definido como parte integrante de la arquitectura IntServ. El funcionamiento del protocolo se puede resumir indicando que cada una de las aplicaciones en el receptor envía un requerimiento de reserva de recursos a la red y ésta podría o bien aceptar o rechazar el pedido. RSVP no transporta datos ni realiza enrutamiento, solo reserva recursos de la red.

2.1.3.3 Modelo DifServ

Gerometta (2010) indica que el modelo DifServ es un modelo de implementación de recursos garantizados de modo genérico y no por flujos o sesiones. Permite garantizar diferentes condiciones de servicio para diferentes tipos de tráfico, de modo escalable y efectivo, a través de toda la red.

- No requiere señalización previa.

- No permite garantizar condiciones de tráfico extremo a extremo.
- Es muy flexible y escalable.
- Divide el tráfico en clases en función de los requerimientos de la organización.
- Cada paquete recibe el tratamiento que se ha definido para la clase a la cual ese paquete pertenece.
- A cada clase se le puede asignar un diferente nivel de servicio y con ello diferentes recursos.
- La asignación de recursos se hace salto por salto en cada dispositivo de la red y no para una ruta específica.
- El mecanismo de implementación es relativamente complejo.

2.1.4 Métodos de Implementación QoS

En los equipos de comunición Cisco, existen 4 métodos para la implementación de calidad de servicio:

2.1.4.1 Método CLI (Command Line Interface)

Una CLI (interfaz de línea de comandos) según Margaret (2015) es una interfaz de usuario para el sistema operativo de un ordenador o una aplicación, en la que el usuario responde a un mensaje visual escribiendo un comando en una línea especificada, recibe una respuesta desde el sistema y entonces entra en otro orden y así sucesivamente.

Este método consume mucho tiempo de procesamiento y tiene mayor probabilidad de cometer errores, ya sean de: digitación, configuración independiente en cada interfaz, cantidad

de código que se desea configurar y otros, lo que lo convierte en uno de los métodos menos recomendados en la actualidad.

Este método fue utilizado años atrás para implementar QoS en los equipos de comunicación, para ello, los pasos de configuración consistían en lo siguiente:

- Identificar, clasificar y priorizar el tráfico.
- Seleccionar la herramienta de calidad de servicio.
- Aplicar la configuración de calidad de servicio en cada interfaz por separado.

2.1.4.2 Método MQC (Modular QoS CLI)

Con el objetivo de evitar algunos inconvenientes producidos por el método CLI, MQC define un nuevo conjuntos de comandos de configuración utilizando el mismo IOS CLI. Este conjunto de comandos de configuración permite configurar la mayoría de características de QoS en los equipos de comunicación como router o switch de manera modular. (Cavanaugh, 2004)

El método de MQC requiere de 3 pasos:

1. **Mapa de Clases:** Definir las clases de tráfico, que representa el primer paso en la implementación de QoS. Las clases son definidas mediante el comando *class map*.

class-map [**match-all** | **match-any**] *map_name*

no class-map [**match-all** | **match-any**] *map_name*

El valor de **match all** define el criterio en los cuales los paquetes cumplen todas las condiciones de la clase, mientras que el valore **match-any** define el criterio en los cuales los paquetes cumplen una sola condición de la clase.

Es comun utilizar listas de control de acceso para realizar la clasificación del tráfico.

Figura 2. 1 Cisco (2015) Configuración de mapa de clase

```
Distribution1(config)#ip access-list extended voice-traffic
Distribution1(config-std-nacl)#permit ip 192.168.100.0 0.0.0.255 any

Distribution1(config-std-nacl)#ip access-list extended
 database-application
Distribution1(config-ext-nacl)#permit tcp any any eq 1521
Distribution1(config-ext-nacl)#permit tcp any any eq 1810
Distribution1(config-ext-nacl)#permit tcp any any eq 2481
Distribution1(config-ext-nacl)#permit tcp any any eq 7778
Distribution1(config-ext-nacl)#exit

Distribution1(config)#class-map  Class-A
Distribution1(config-cmap)#match access-group name voice-traffic
Distribution1(config-cmap)#exit
Distribution1(config)#class-map  Class-B
Distribution1(config-cmap)#match access-group name
 database-application
Distribution1(config-cmap)#exit
```

2. **Mapa de Política:** Definir las políticas de QoS para las clases. Varias clases pueden ser asociados a una política y varias políticas pueden ser definidas. Las políticas son definidas mediante el comando *policy-map.*

policy-map *policy-map-name*

no policy-map *policy-map-name*

Para poder realiza la asociación de una o varios mapas de clase dentro del mapa de política se utiliza el comando *class* dentro de la configuración del mapa de política.

(config-pmap)# **class** *class_map_name*

Figura 2. 2 Cisco (2015) Configuración de mapa de política

Figura 2. 3 Cisco (2015) Configuración de mapa de política

Figura 2. 4 Cisco (2015) Configuración de mapa de política

```
Distribution1(config)#policy-map sample-policy1
Distribution1(config-pmap)#class Class-A
Distribution1(config-pmap-c)#trust cos
Distribution1(config-pmap-c)#exit
Distribution1(config-pmap)#class Class-B
Distribution1(config-pmap-c)#set dscp af21
Distribution1(config-pmap-c)#exit
Distribution1(config-pmap)#exit
```

3. **Política:** Aplicar la política de servicio. La pólitica de servicio podrá ser aplicada a las interfaces de entrada como de salida, utilizando el comando *service-policy*.

service-policy {input | output} *policy-map-name*

no service-policy {input | output} *policy-map-name*

Figura 2. 5 Cisco (2015) Configuración de política

```
Distribution1(config)#interface gigabitEthernet 1/0/13
Distribution1(config-if)#switchport access vlan 10
Distribution1(config-if)#switchport mode access
Distribution1(config-if)#switchport voice vlan 100
Distribution1(config-if)#spanning-tree portfast
Distribution1(config-if)#service-policy input sample-policy1
Distribution1(config-if)#exit
```

MQC es un método recomendado y el más poderoso para la implementación de QoS. Es modular, promueve la reutilización de código escrito y facilita la compatibilidad de la configuración de QoS entre dispositivos de Cisco. MQC también reduce las posibilidades de errores y conflictos, y le permite tomar ventaja de las últimas características y mecanismos ofrecidos por las versiones de Cisco IOS. (In Depth Tutorials and Information)

2.1.4.3 Auto QoS

Cisco Systems (2015) señala que AutoQoS es una tecnología innovadora de Cisco, que reduce al mínimo la complejidad, tiempo y costo de operación de implementación de la calidad de servicio. AutoQoS de Cisco incorpora inteligencia de valor agregado en el Software Cisco IOS y en el software del Cisco Catalyst para el funcionamiento, provisionamiento y administración de implementaciones a gran escala de calidad de servicio.

Cisco Systems (2015) señala los siguientes beneficios al utilizar Auto QoS durante las implementaciones:

- Cisco AutoQoS simplifica la implementación de QoS y acelera la provisión de tecnología de calidad de servicio sobre una infraestructura de red de Cisco. Se reduce el error humano y reducen los costos de capacitación. Con AutoQoS-VoIP, un comando puede habilitar QoS para VoIP en cada enrutador y switch. El usuario también puede modificar los política/comandos AutoQoS generados mediante la CLI para cumplir requisitos específicos.
- Las empresas pueden beneficiarse de los costos de implementación y tiempo, que son hasta tres veces más baratos y más rápidos que un enfoque manual. Se puede utilizar plantilla enfocada a AutoQoS para reducir los gastos operacionales.

Para la implementación o uso de AutoQoS en una interface de un enrutador o switch es necesario que se encuentren habilitandas las siguientes opciones:

1. **CEF** (***Cisco Express Forwarding***): Permite que el proceso de conmutación de tráfico sea más rápido. A partir de la habilitación de CEF es posible habilitar las funciones

avanzadas como NBAR. CEF se habilita utilizando el comando *ip cef* dentro de las configuraciones del enrutador o switch.

Router(config)# **ip cef**

2. **NBAR (*Network Based Application Recognition)***: Proporciona el reconocimiento automatico de aplicaciones basados en red y provee apropiados mecanismos de QoS. NBAR se habilita utilizando el comando *ip nbar protocol-discovery* dentro de la interface que se desea clasificar y marcar el tráfico.

Router(config-if)# **ip nbar protocol-discovery**

3. **Ancho de Banda:** Es importante que dentro de la interface al cual será aplicado Auto QoS este corectamente configurado el ancho de banda. El ancho de banda se configura utilizando el comando *bandwidth* dentro de la interface en la cual se aplicará AutoQos.

Auto QoS se habilita utilizando el siguiente comando *auto qos* dentro de la interface a la cual se desea aplicar.

Switch(config-if)# **auto qos [voip | video | classify | trust]**

Figura 2. 6 Trejo (2015) Configuración de Auto QoS

```
Router(config)#ip cef
Router(config)#interface serial0/0
Router(config-if)#bandwidth 2000000
Router(config-if)#auto qos voip
```

2.1.4.4 SDM (Security Device Manager) QoS Wizard

Cisco SDM es una herramienta de administración de dispositivos basada en web para los equipos Cisco, simplificando la solución de problemas de red y conectividad, adicionalmente, proporciona asistentes inteligentes que ayudan a realizar la configuración de interfaces, NATs, firewall, vpn, paso a paso.

El asistente de QoS de SDM proporciona las siguientes características:

- Una interfaz de usuario fácil de usar para definir las clases de tráfico y configurar las directivas de QoS de la red.
- Predefine tres categorías de aplicaciones diferentes: real time, misión crítica y best effort.
- Admite y utiliza NBAR para validar el ancho de banda consumido por las categorías de las aplicaciones.
- Implementar, monitorear y resolver problemas en QoS en la red.

A continuación se detalla el acceso hacia la interfaz SDM y la configuración del wizard de SDM para calidad de servicio:

Figura 2. 7 Cisco System (2007) Security Device Manager (SDM)

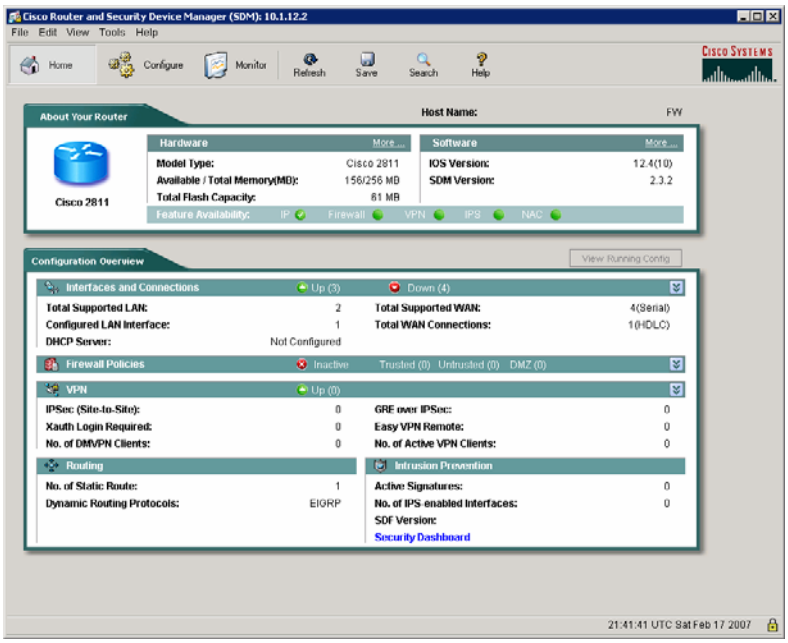


Figura 2. 8 Cisco System (2007) Política de craciόn de QoS

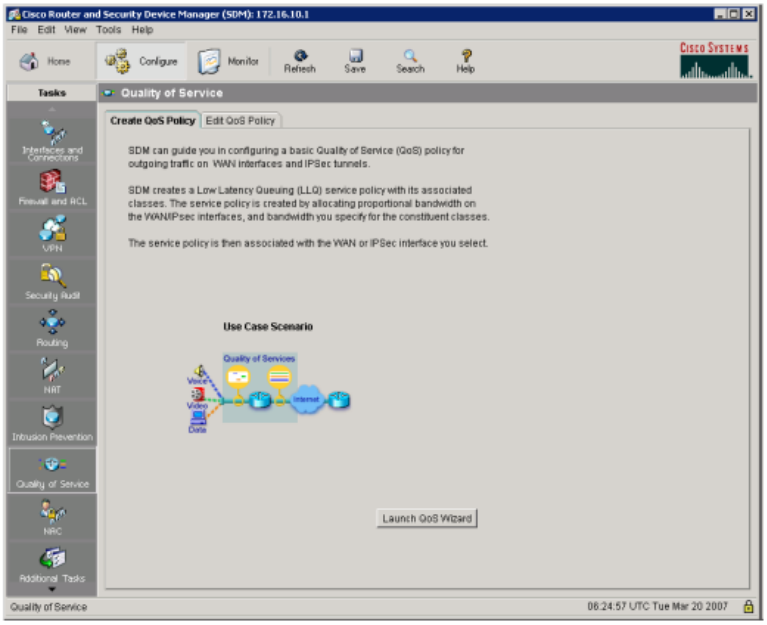


Figura 2. 9 Cisco System (2007) Asistente de QoS SDM

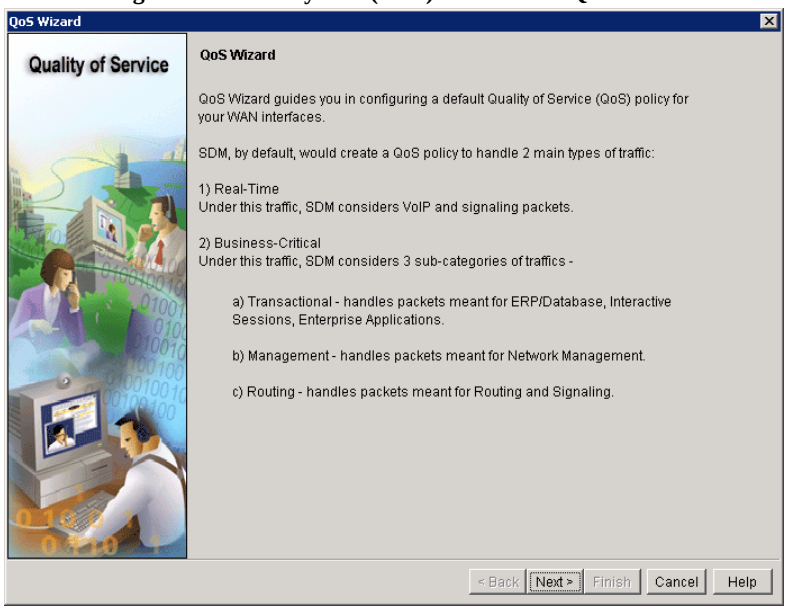


Figura 2. 10 Cisco System (2007) Asistente de QoS SDM - Interface

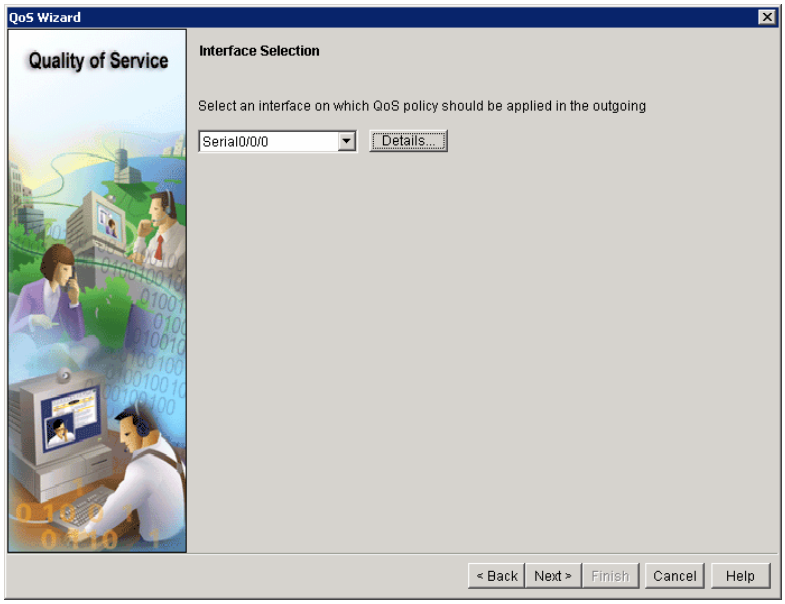


Figura 2. 11 Cisco System (2007) Asistente de QoS SDM - Generación de política de QoS

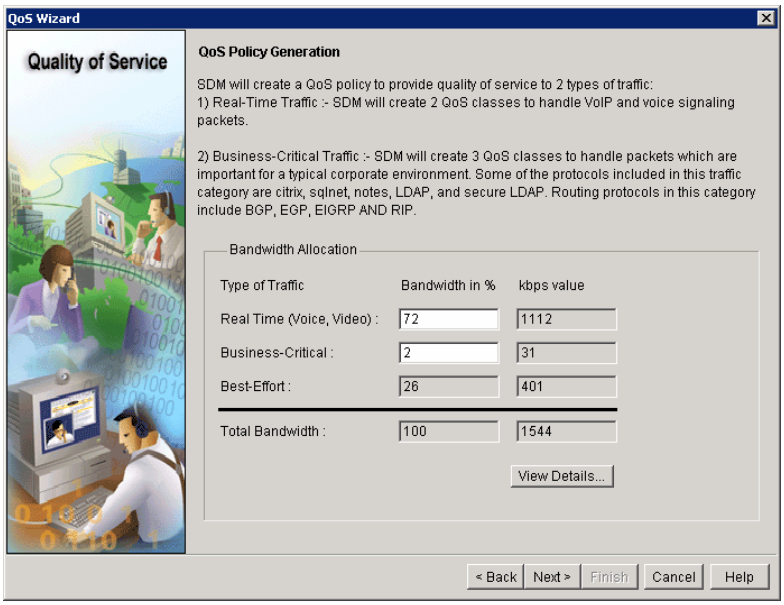
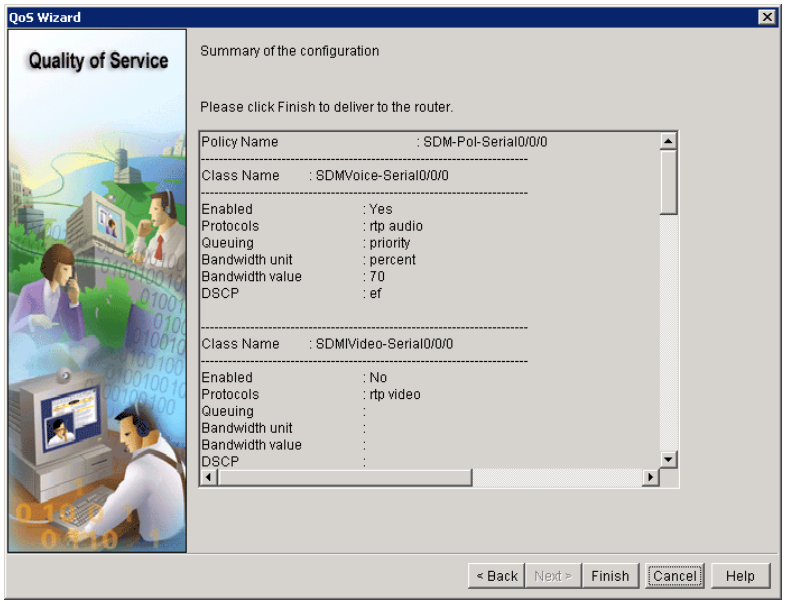


Figura 2. 12 Cisco System (2007) Asistente de QoS SDM - Parametros de configuración



La Tabla 1.1 muestra una comparación de los métodos de implementación de QoS evaluados por los siguientes criterios:

Tabla 2. 1 Comparación de métodos de implementación de QoS

	CLI	MQC	Auto QoS	SDM
Facilidad de Uso	Más Dificil	Más Fácil que CLI	Simple	Simple
Capacidad de precisión.	Menor	Buena	Limitada	Limitada
Implementación y consumo de tiempo	Mayor	Moderado	Menor	Menor
Modularidad	Muy Pobre	Muy Modular	Muy modular	Bueno

2.2 Clasificación y Marcaje

Para realizar la implementación de QoS es necesario dar un tratamiento especial a todos los tipos y clases de tráfico de red. Este tratamiento consiste en la clasificación y marcaje.

2.2.1 Clasificación

"Clasificación es el proceso o mecanismo que identifica el tráfico y permite categorizar a este en clases" (Wong, 2012).

La clasificación permite que los diferentes tipos de tráfico no sean considerados como tráfico Best Effort, por ello es considerado como el mecanismo fundamental en la implementación de qos y es recomendable se lo realice en los puntos más cercanos a las fuentes de tráfico.

Los mecanismos más utilizados para realizar la clasificación son:

- **ACL (Listas de Control de Acceso):** Las Listas de Control de Acceso tienen como objetivo permitir o denegar el tráfico y filtrar el tráfico.
- **NBAR (Network Based Application Recognition):** NBAR es un aplicación propietaria de CISCO que tiene como objetivo la clasificación del tráfico, descubrimiento de protocolos y presentación de estadísticas del tráfico. NBAR será aplicado en el desarrollo del capitulo 3 en el levantamiento del tipo de tráfico de la Unidad de Negocios Termopichincha.

Cisco (2015) afirma que la clasificación de paquetes implica el uso de un descriptor del tráfico para categorizar un paquete dentro de un grupo específico.

2.2.1.1 Descriptores de Tráfico

Los descriptores de tráfico son datos específicos que posee un paquete y los diferencia de los otros, permitiendo obtener una clasificación específica del paquete. Estos descriptores pueden ser:

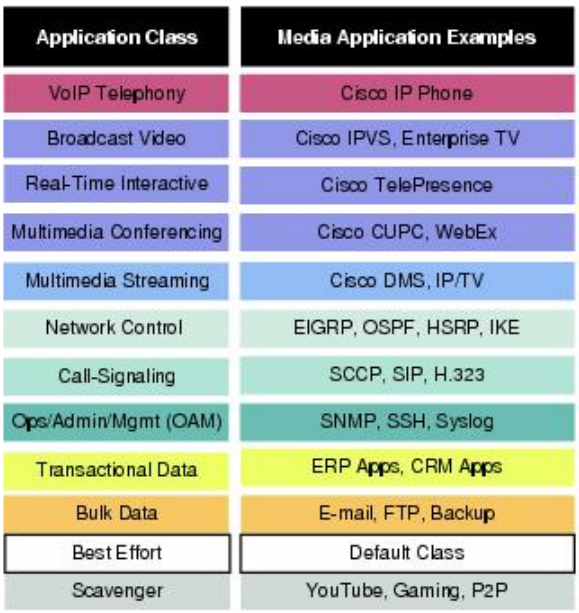
- Valor de CoS en la trama
- Campo IP Precedence en la cabecera del paquete IP
- Valor DSCP del la cabecera del paquete IP
- Valor MPLS EXP de la cabecera MPLS

- Direcciones IP del origen y destino del paquete IP

2.2.1.2 Clases de Tráfico

Dependiendo de los descriptores de tráfico utilizados y de las mejores prácticas de calidad de servicio, la figura muestra una clasificación recomendada del tráfico.

Figura 2. 13 (Rahul Kachalia, Cisco Systems, 2010) Clases Recomendadas



Application Class	Media Application Examples
VoIP Telephony	Cisco IP Phone
Broadcast Video	Cisco IPVS, Enterprise TV
Real-Time Interactive	Cisco TelePresence
Multimedia Conferencing	Cisco CUPC, WebEx
Multimedia Streaming	Cisco DMS, IP/TV
Network Control	EIGRP, OSPF, HSRP, IKE
Call-Signaling	SCCP, SIP, H.323
Ops/Admin/Mgmt (OAM)	SNMP, SSH, Syslog
Transactional Data	ERP Apps, CRM Apps
Bulk Data	E-mail, FTP, Backup
Best Effort	Default Class
Scavenger	YouTube, Gaming, P2P

2.2.1.2.1 Clase VoIP

Clase que identifica al tráfico de telefonía IP, que requiere la provisión de prioridad muy alta y ancho de banda garantizado y evitar que sea afectado por la pérdida de paquetes, latencia y jitter, manteniendo una comunicación clara y sin cortes. Ejemplos los codecs G.711 o G.729.

2.2.1.2.2 Clase Multimedia

Clase que identifica al tráfico relacionado con aplicaciones de video en tiempo real, aplicaciones de colaboración de multimedia en donde la prioridad principal es el video y la voz (videoconferencia) y el video bajo demanda (streaming), que requieren de un provisión de prioridad alta y ancho de banda garantizado y evitar que sea afectado por la perdida de paquetes y latencia. Ejemplo Sistemas de Video Conferencia Polycom, WebEx.

2.2.1.2.3 Clase Tráfico de Señalización

Clase que identifica al tráfico relacionado con señalización de voz (telefonía) y video, y tráfico de control de redes necesarios para la operación de la infraestructura de red. Evitar la perdida de paquete en cuanto a la voz permitirá establecer correctamente la comunicación de telefonía IP entre sitios.

2.2.1.2.4 Clase de Aplicaciones Transaccionales

Clase que identifica al tráfico de aplicaciones críticas para el negocio y afectan directamente a los usuarios ya que son utilizadas diariamente. Evitar la latencia de los aplicativos transaccionales conlleva a una mayor productividad para los usuarios sin afectar a la operación normal, manteniendo tiempos de respuesta adecuados dentro de la red. Ejemplos Sistemas ERP.

2.2.1.2.5 Clase de Aplicaciones No Transaccionales

Clase que identifica al tráfico de aplicaciones menos críticas para el negocio y que no afectan directamente a los usuarios en sus operaciones normales.

2.2.1.2.6 Clase Best-Effort

Clase que identifica al tráfico que no es identificado en ninguna de las clases antes mencionadas. Es una clase que existe por defecto y la gran mayoría de las aplicaciones serán identificadas de esta manera.

2.2.1.2.7 Clase Scavenger

Clase que identifica al tráfico basura, que no tiene ninguna relación con el negocio.

2.2.2 Marcaje

Luego de la primera etapa, en la cual se realiza la clasificación de los paquetes, continua la segunda etapa que comprende el proceso de marcaje, permitiendo marcar con un identificador los paquetes o tramas e identificarlos dentro de las distintas clases. Cuando los paquetes son marcados, los distintos mecanismos de QoS pueden realizar la clasificación de los paquetes únicamente analizando las cabeceras.

El marcaje de los paquetes involucra realizar cambios en la configuración de algunos bits dentro de la cabecera, que pueden ser aplicados tanto en la capa de enlace de datos como en la capa de red. Es recomendado realizar el marcaje en la capa de red debido a que si el paquete es marcado en la capa de enlace de datos, la cabecera puede ser eliminada durante su recorrido, mientras que en la capa de red no se altera.

Es importante tener en cuenta que el marcaje debe realizarse dentro del perímetro de la red en el cual los dispositivos confian y respetan el marcaje realizado. Este perímetro es conocido como

"Trust Boundary". Si los paquetes fueron marcados fuera del perímetro, pueden ser remarcados por otro dispositivo ocasionando que la clasificación cambie.

Los marcajes más comunes en la capa de enlace de datos son: CoS (Class of Service) en Ethernet, EXP (Experimental) en MPLS, DE (Discard Elegible) en Frame Relay, CLP (Cell Loss Ptiority) en ATM, y en la capa de red: IP Precedence y DSCP.

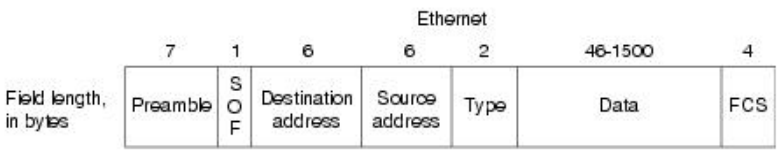
2.2.2.1 Capa Enlace de Datos

La función de la capa de enlace de datos es preparar los paquetes de la capa de red para ser transmitidos y controlar el acceso a los medios físicos, es decir que se encarga del direccionamiento físico, del acceso al medio, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo. (Bravo, 2011)

En el caso de la comunicación entre equipos de capa 2, Ethernet presenta dos mecanismos de QoS para la clasificción y marcaje conocidos como IEEE 802.1q y IEEE 802.1p. IEEE 802.1q permite añadir etiquetas para el tratamiento de VLAN en comunicación troncalizada y IEEE 802.1p que presenta distintas clases de servicio. Se podría decir que dentro de la cabecera que conforma IEEE 802.1q se encuentra inverso el IEEE 802.1p.

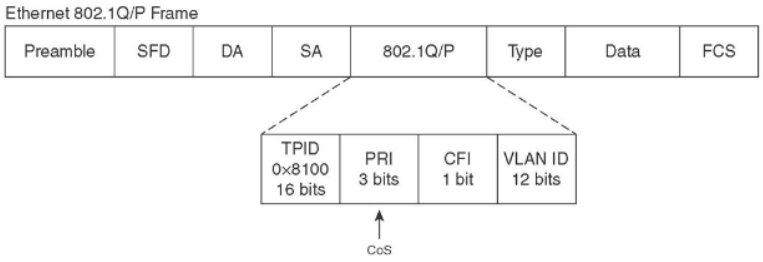
La figura 2.12 muestra el formato de ethernet y los campos que lo conforman.

Figura 2. 14 (Cisco Systems, 2015) Formato Ethernet



IEEE 802.1q. esta conformado por 4 bytes que son añadidos dentro de la trama ethernet según se muestra en la figura 2.13.

Figura 2. 15 (What-When-How) Formato de la trama Ethernet añadido 802.1 Q



Como se observa introduce un encabezado de 4 bytes dentro del encabezado Ethernet después de la dirección MAC origen. Los primeros 12 bits del encabezado de etiqueta especifican el VLAN ID, permitiendo de esta manera 4095 VLANs individuales. El campo Canonical Format Indicator (CFI, Indicador de Formato Canónico) le corresponde 1 bit, este cuando está en off indica que el dispositivo debe leer la información de la trama en forma canónica (de derecha a izquierda), la razón de este bit es que 802.1q puede utilizar tramas Token Ring o Ethernet, un dispositivo siempre lee de forma canónica, pero los Token Ring no, por eso para una trama Ethernet este valor es "0". Para el campo User Priority se utilizan 3 Bits, y este se refiere a la prioridad de la trama por razón de calidad de servicio CoS. Y por último el campo Tag Protocol ID (ID del protocolo de VLAN), a este campo se le asignan 2 bytes, especifica que es una trama etiquetada, señala el cambio en el formato de la trama. (Gómez)

2.2.2.1.1 Cos (Class Of Service)

IEEE 802.1p es un estándar que define niveles de prioridad CoS diferentes para el campo User Priority de la figura 2.13. Cuando se envían los paquetes clasificados por prioridad según este estándar a la red, los dispositivos preparados para IEEE 802.1p transfieren los paquetes con mayor prioridad, además cuando se produce congestión de la red, los paquetes que se consideren de mayor prioridad recibirán un trato preferencial, mientras que los paquetes de baja prioridad se mantendrán en suspenso. (Gómez)

IEEE 802.1.p permite clasificar en 8 tipos de tráficos como se muestra en la figura 2.14, siendo el valor de 0 el de menor importancia (tráfico Best-Effort).

Figura 2. 16 (Cisco Systems, 2007) Clasificación de Tráfico CoS

2.2.2.1.2 MPLS EXP

MPLS (Multiprotocol Label Switching) es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las

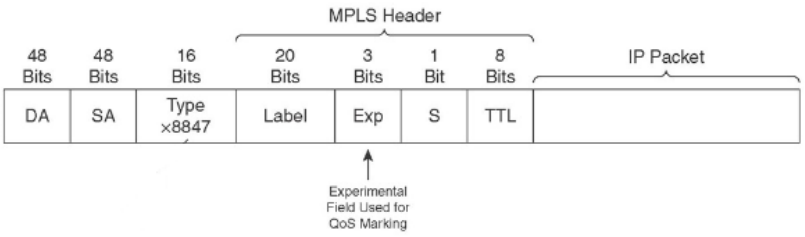
redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP. (Wikipedia, 2015)

MPLS es una tecnología de reenvío de paquetes que utiliza las escrituras de la etiqueta para tomar las decisiones del reenvío de datos. Con MPLS, el análisis del encabezado de la capa 3 se hace apenas una vez cuando el paquete ingresa el dominio MPLS. MPLS proporciona aplicaciones beneficiosas como Virtual Private Networking (VPN), Ingeniería de tráfico (TE), Calidad del servicio (QoS), y cualquier transporte sobre MPLS. Las tecnologías MPLS son aplicables a cualquier protocolo de capa de red. (Cisco Systems, 2015)

Dentro de la cabecera que conforma MPLS de 4 bytes se encuentra definido el campo EXP (Experimental) que se refiere a la prioridad de la trama por razón de calidad de servicio CoS, permitiendo diferencias en 8 tipos de tráfico mediante 3 bits según la figura 2.14.

La figura 2.15 muestra la cabecera de MPLS con el campo EXP.

Figura 2. 17 (What-When-How) Cabecera MPLS



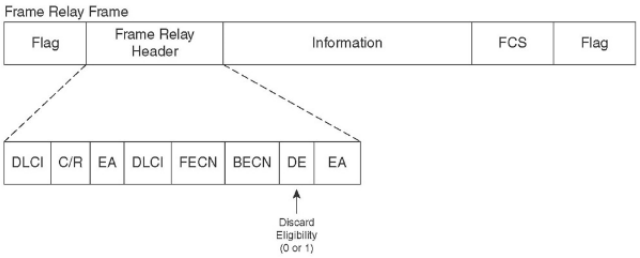
2.2.2.1.3 Frame Relay bit DE (Discard Elegibility)

Frame Relay (Frame-mode Bearer Service) es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o

marcos (“frames”) para datos, perfecto para la transmisión de grandes cantidades de datos. (Wikipedia, 2015)

En el caso de Frame Relay no existe un campo que sea definido para el CoS, peo dentro de su cabecera existen 2 campos llamados FECN (Forward Explicit Congestion Notification) y BECN (Backward Explicit Congestion Notification) que permiten realizar la prevencion de la congestión y el campo DE (Discard Elegibility) que maneja la probabilidad de descarte de los paquetes.

Figura 2. 18 (What-When-How) Cabecera de Frame Relay



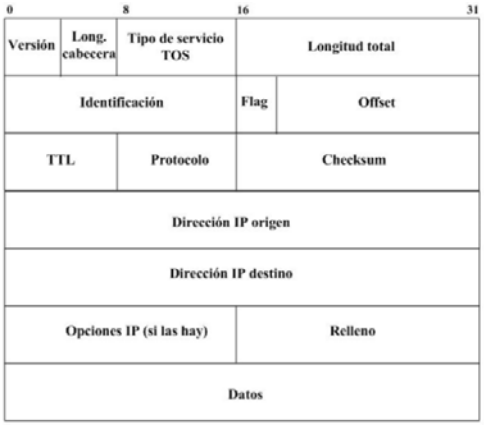
2.2.2.2 Capa de Red

La capa de red proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Es el tercer nivel del modelo OSI y su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa. Ofrece servicios al nivel superior (nivel de transporte) y se apoya en el nivel de enlace, es decir, utiliza sus funciones. (Wikipedia, 2015)

En el caso de la capa de red, para poder diferenciar lo paquetes es necesario realizar el marcaje y clasificación, para este propósito el datagrama del protocolo IP cuanta con el campo

ToS (Type of Service). Como se muestra en la figura 2.17, el campo ToS esta compuesto por 8 bits y define la calidad de servicio del datagrama IP.

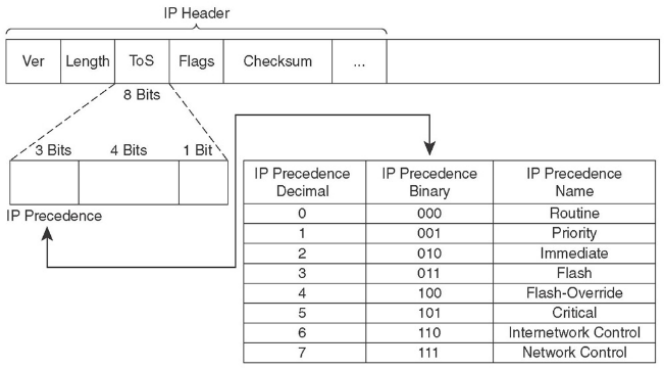
Figura 2. 19 Datagrama IP



2.2.2.2.1 IP Precedence

Con la necesidad de aplicar calidad de servicio dentro del campo ToS de 8 bits de IP, se define un tipo de marcaje mediante la utilización de los 3 bits más significativos llamado IP Precedence. Entre mayores sean los valores de IP Precedence el paquete es marcado con la mayor prioridad. En la figura 2.18 muestra el campo ToS y los valores correspondientes a IP Precedence.

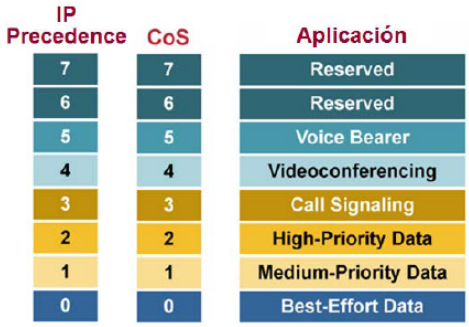
Figura 2. 20 (What-When-How) ToS y valores IP Precedence



IP Precedence Decimal	IP Precedence Binary	IP Precedence Name
0	000	Routine
1	001	Priority
2	010	Immediate
3	011	Flash
4	100	Flash-Override
5	101	Critical
6	110	Internetwork Control
7	111	Network Control

En la figura 2.19 se puede observar que los valores del IP Precedence están muy relacionados con los valores de CoS del estandar IEEE 802.1p. Esto permite manejar compatibilidad asegurando una consistencia en la comunicación end-to-end.

Figura 2. 21 Valores IP Precedence y CoS



2.2.2.2.2 DSCP

Con la necesidad de aplicar mejoras en la calidad de servicio dentro del campo ToS de 8 bits de IP, se define un tipo de marcaje mediante la utilización de los 6 bits llamado DSCP. Differentiated Services Code Point permite diferenciar la calidad de servicios que se manejaran en la comunicación y es considerado el método estandar en marcado de tráfico IP.

Figura 2. 22 (Cisco System, 2006) DSCP

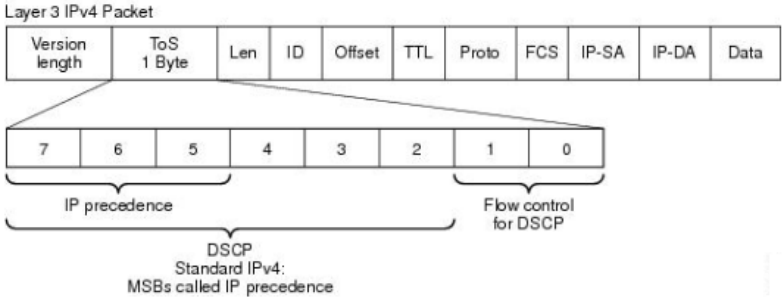
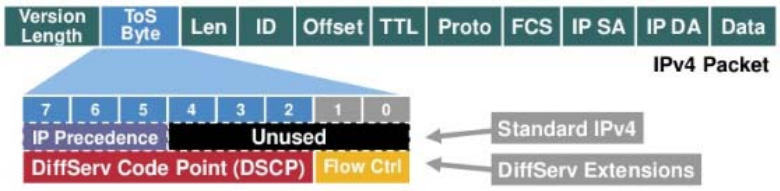
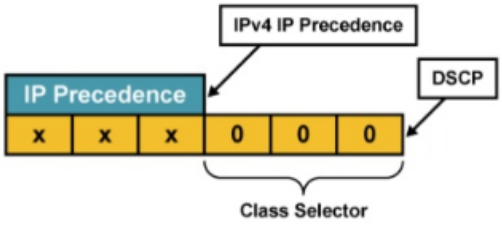


Figura 2. 23 (Cisco Systems, 2007) IP Precedence y DSCP



Redefiniendo, el byte ToS es el campo de servicios diferenciados (DiffServ) revisado en el capitulo 2 de los Modelos de QoS, con los 6 bits más significativos llamados DSCP, ha proporcionado mucha más flexibilidad y capacidad para aplicar calidad de servicio en IP. DSCP es compatible con las prioridades definidas en IP Precedence, proporcionando la oportunidad para el despliegue gradual de la base de DSCP QoS en redes IP. (What-When-How)

Figura 2. 24 (Cisco Systems, 2007) Compatibilidad de IP Precedence y DSCP



El punto de código DS (DSCP) define en el encabezado del paquete la acción que cualquier sistema con Diffserv debe ejecutar en un paquete marcado. La arquitectura Diffserv define un conjunto de puntos de código DS que utilizarán los sistemas con IP QoS y enrutadores Diffserv. La arquitectura Diffserv también define un conjunto de acciones denominadas comportamientos de reenvío, que corresponden a los DSCP. El sistema IP QoS marca los bits precedentes del campo DS del encabezado del paquete con el DSCP. Cuando un enrutador recibe un paquete con un valor DSCP, aplica el comportamiento de reenvío asociado a dicho DSCP. Después, el paquete se envía a la red. En la terminología Diffserv, el comportamiento de reenvío asignado a

un DSCP se denomina comportamiento por salto (PHB). El PHB define la precedencia de reenvío de un paquete marcado que recibe en relación con otro tráfico del sistema con Diffserv. Esta precedencia determina si el sistema con IP QoS o enrutador Diffserv reenvía o descarta el paquete marcado. Para un paquete reenviado, cada enrutador Diffserv que el paquete encuentra en la ruta hasta su destino aplica el mismo PHB. La excepción ocurre si otro sistema Diffserv cambia el DSCP. (Oracle Corporation, 2010)

El objetivo de PHB es proporcionar una cantidad específica de recursos de red a una clase de tráfico en la red contigua. Puede conseguir este objetivo en la directiva QoS. Define los puntos DSCP que indican los niveles de precedencia para las clases de tráfico cuando los flujos de tráfico abandonan el sistema con IP QoS. Las precedencias pueden alternar entre alta precedencia/baja probabilidad de descarte y baja precedencia/alta probabilidad de descarte. (Oracle Corporation, 2010).

2.2.2.2.2.1 Tipos de PHB

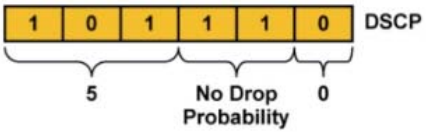
DSCP presenta 4 tipos de niveles de precedencia de reenvío para las clases de tráfico:

- Por defecto
- EF
- AF

1. **Por Defecto:** El valor de DSCP es 000 indicando que no se encuentra asignado ningún valor de PHB. El tratamiento del tráfico sigue la condición de primero en entrar, primero en salir (FIFO), por ello no aplica ningún mecanismo de calidad de servicio. En este caso, no se da ningún tratamiento especial al tráfico que paso por un nodo.

2. **EF (Expedited Forwarding):** El reenvío acelerado indica que los valores de DSCP son los más altos, con la mayor prioridad, permitiendo que el paquete presente la menor probabilidad de descarte y garantizando un retardo y ancho de banda mínimo. El valor de DSCP es 101110.

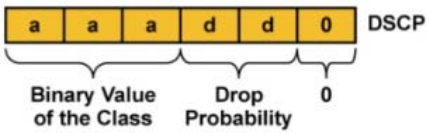
Figura 2. 25 (Cisco Systems, 2007) EF PHB



La combinación de los valores esta definida de la siguiente manera: Los 3 primeros bits 101 = 5 de IP Precedence, los 2 bits siguientes 11 indican la probabilidad de descarte y el ultimo bit es 0.

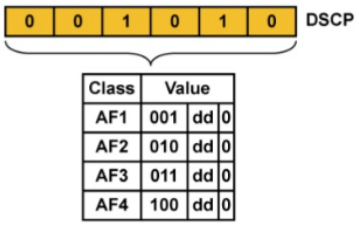
3. **AF (Assure Forwarding):** El reenvío asegurado indica que los valores de DSCP son diferenciados por 4 clases: AF1, AF2, AF3 y AF4, los cuales permiten brindar distintos niveles de prioridad, garantizar ancho de banda y probabilidad de descarte de los paquetes.

Figura 2. 26 (Cisco Systems, 2007) AF PHB



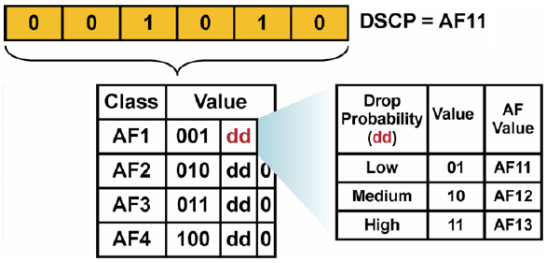
La combinación de los valores esta definida de la siguiente manera: Los 3 primeros bits aaa es el valore binario de la clase, los 2 bits siguientes dd indican la probabilidad de descarte y el ultimo bit es 0.

Figura 2. 27 (Cisco Systems, 2007) Clases AF PHB



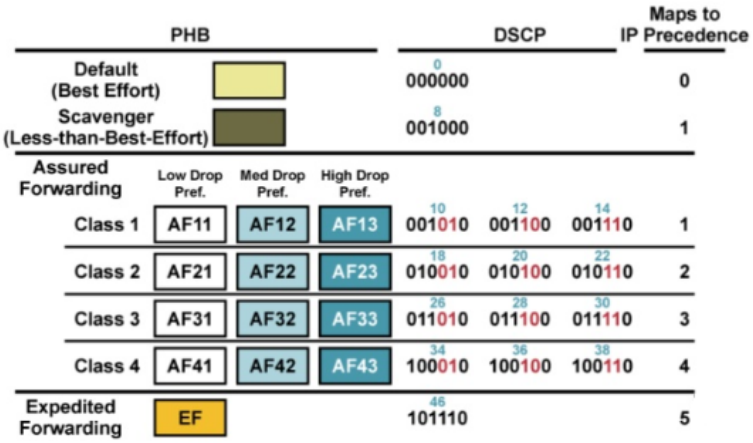
Los 2 bits de la probabilidad de descarte (dd) permiten manejar tres combinaciones distintas por cada clase, las cuales serán tratadas de manera independiente dando diversas prioridades a los paquetes a nivel de la probabilidad del descarte.

Figura 2. 28 (Cisco Systems, 2007) Combinaciones por Clase AF



La figura 2.27 muestra una tabla sobre los distintos tipos de PHB con la clasificación de los valores de AF, con los valores DSCP e IP Precedence correspondientes.

Figura 2. 29 (Cisco Systems, 2007) PHB - DSCP - IP PRECEDENCE



La figura 2.28 muestra la clasificación y marcaje recomendado por Cisco para las distintas aplicaciones a nivel de capa de red y capa de enlace de datos revisadas anteriormente.

Figura 2. 30 (Cisco Systems, 2007) Clasificación y Marcaje Cisco

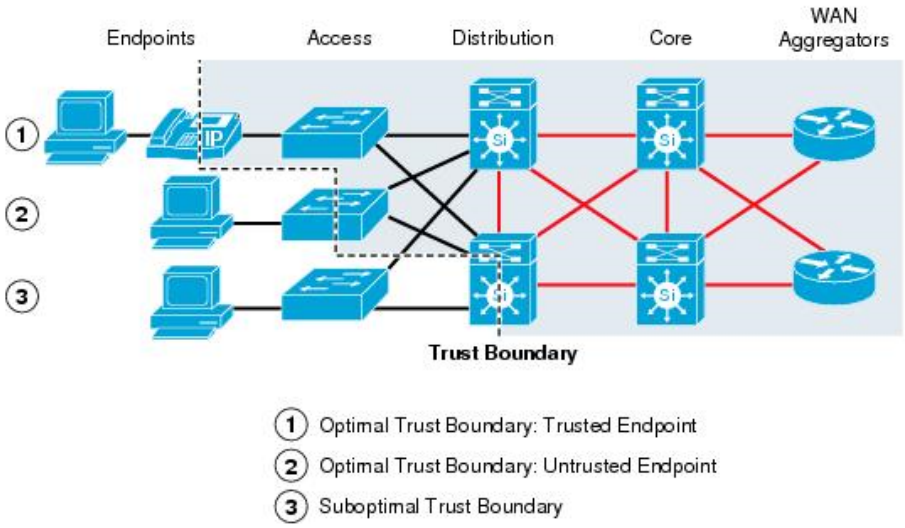
Application	L3 Classification			L2
	IPP	PHB	DSCP	CoS
Routing	6	CS6	48	6
Voice	5	EF	46	5
Video Conferencing	4	AF41	34	4
Streaming Video	4	CS4	32	4
Mission-Critical Data	3	AF31*	26	3
Call Signaling	3	CS3*	24	3
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1
Scavenger	1	CS1	8	1
Best Effort	0	0	0	0

2.2.3 Trust Boundary

Cisco (2014) indica que un límite de confianza es el punto dentro de la red donde las marcas como CoS o DSCP comienzan a ser aceptadas y depende de las capacidades de los extremos que están conectados al borde de acceso de la LAN.

Para que los límites de confianza puedan ser establecidos y cumplidos dentro de los limites de la red y por los dispositivos que lo conforman, se definen 3 modelos de confianza: extremos de confianza, extremos de no confianza y extremos de confianza condicionales.

Figura 2. 31 (Cisco System, 2006) Limites de Confianza



Con relación a la figura 2.29, el primer modelo de extremos de confianza nos muestra que los límites de confianza son definidos a partir del dispositivo más cercano a la fuente de tráfico, en este caso, el telefono IP va a marcar todo el tráfico que será enviado al dispositivo de acceso. En el segundo modelo de extremos de no confianza nos muestra que los límites de confianza son definidos a partir del dispositivo más cercano a la fuente de tráfico, en este caso, el switch de acceso va a marcar todo el tráfico dependiendo de las capacidades del switch que será enviado al dispositivo de distribución y no confiará en nada antes de este. En el tercer modelo de extemos de confianza condicional nos muestra que los límites de confianza son definidos lo más lejano a la fuente de tráfico, en este caso, el switch de distribución va a marcar todo el tráfico, mapea CoS a ToS (IP precedence) o a DSCP y no confiará en nada antes de este. Este modelo no es muy usado ya que implica no confiar en los dispositivos de acceso.

2.2.4 NBAR

Network Based Application Recognition es una funcionalidad propietaria de Cisco la cual permiten a los IOs de los equipos Cisco realizar tareas importantes como: el reconocimiento de protocolos, mostrar la información estadística de toda la información recopilada de los protocolos y la clasificación del tráfico.

Estas tareas dentro de los equipo router pueden producir sobrecarga de trabajo en el CPU del equipo, dependiendo de la cantidad de tráfico que pasa por el equipo. NBAR tiene un reconocimento limitado de protocolos dependiendo de la cantidad de PDLMs que posea el equipo.

NBAR posee algunas limitaciones como:

- No funciona en interfaces con Fast EtherChannel.
- Analiza unicamente los primeros 400 bytes del paquete.
- Funciona unicamente cuando CEF está activo. CEF Permite que el proceso de conmutación de tráfico sea más rápido.
- No analiza paquetes fragmentados.
- Reconocimiento limitado y depende de los PDLMs para expandir su renocimiento.

NBAR posee algunas ventajas como:

- Herramienta muy poderosa y simple para realizar la clasificación y marcaje.
- Maneja una clasificación basada en el contenido de la aplicación.
- Clasificación basada en los numeros de los puertos estáticos y dinámicos de TCP y UDP.

Cisco Systems (2016) indica que cuando NBAR reconoce y clasifica un protocolo o aplicación, la red puede configurarse adecuada para aplicar calidad de servicio (QoS) para esa aplicación o tráfico con ese protocolo.

En la siguiente Tabla 2.2 se pueden observar los diferentes puertos tanto TCP como UDP que NBAR puede reconocer:

Tabla 2. 2 Datos NBAR obtenidos en la red de Termopichincha

Protocolos	
http	h323
ssl	sip
cifs	icmp
notes	ping
rtcp	snmp
video-over-http	sqlserver
secure-http	oracle-sqlnet
imap	webex-meeting
smtp	ftp
rtp	active-directory
rtmp	ldap
dnp	pop3
dns	

2.2.4.1 PDLMs

Packet Description Language Modules permite ampliar la lista de protocolos que NBAR puede reconocer, mejorando una de las limitaciones al utilizar NBAR.

PDLMs son archivos que Cisco Systems publica, estos archivos contienen reglas que NBAR emplea para reconocer protocolos y aplicaciones. Un nuevo PDLM puede ser cargado en la memoria flash del dispositivo Cisco y luego se hace referencia dentro de su configuración sin necesidad de realizar una actualización al IOS o cargar el dispositivo. (What-When-How)

Los NBAR realiza el reconocimiento y clasificación de los paquetes basado en el analisis y comparación de las reglas definidas en los Móulos de lenguaje de descripción de protocolos.

Los comandos que permite subir PDLM al IOS de los equipos Cisco que soportan NBAR son los siguientes:

- *Router>* **enable**
- *Router#* **configure terminal**
- *Router(config)#* **ip nbar pdlm *pdlm-name*** (pdlm-name es el nombre del archivo que se encuentra en la Flash://ruta url)

2.2.4.2 Protocol Discovery

Una de las funcionalidades de NBAR es el Descubrimiento de Protocolos, que proporciona una manera fácil de descubrir las aplicaciones o protocolos que funcionan en una interfaz. Se puede descubrir cualquier tráfico de protocolo que admite NBAR y obtener estadísticas que se asocian con dicho protocolo, que luego pueden utilizarse para definir las clases y las políticas de tráfico, y aplicar características especificas de QoS (Cisco Systems, 2016). Las estadísticas presentan información de:

- Número total de bytes y de paquetes de entrada
- Número total de salida de paquetes y bytes

- Tasas de bits de entrada
- Tasas de bits de salida

El descubrimiento de protocolos es aplicado en tiempo real, obteniendo información de manera inmediata sobre los aplicativos o protocolos que ese momento se encuentran cruzando en puntos definidos de la red.

Los comandos necesarios para habilitar Protocol Discovery en una interfaz son los siguientes:

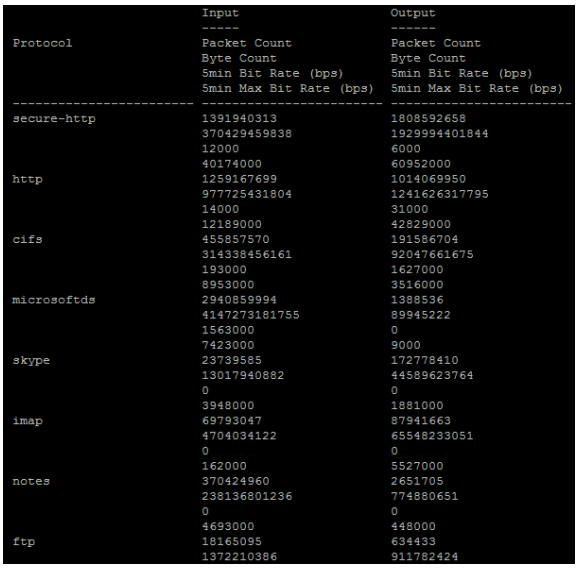
- *Router>* **enable**
- *Router#* **configure terminal**
- *Router(config)#* **ip cef** (necesario para que funcione NBAR)
- *Router(config)#* **interface Giga o FastEthernet #/#**
- *Router(config-if)#* **ip nbar protocol-discovery**
- *Router(config-if)#* **end**

Para visualizar los resportes estadísticos obtenidos al habilitar **nbar protocol-discovery**, se debe utilizar el siguiente comando:

- *Router#* **show ip nbar protocol-discovery**

La figura 2.30 muestra un ejemplo de la información que se despliega al ejecutar el comando anterior.

Figura 2. 32 Estadísticas Protocol Discovery - Router Termopichincha



	Input	Output
	-----	------
Protocol	Packet Count	Packet Count
	Byte Count	Byte Count
	5min Bit Rate (bps)	5min Bit Rate (bps)
	5min Max Bit Rate (bps)	5min Max Bit Rate (bps)
secure-http	1391940313	1808592658
	370429459838	1929994401844
	12000	6000
	40174000	60952000
http	1259167699	1014069950
	977725431804	1241626317795
	14000	31000
	12189000	42829000
cifs	455857570	191586704
	314338456161	92047661675
	193000	1627000
	8953000	3516000
microsoftds	2940859994	1388536
	4147273181755	89945222
	1563000	0
	7423000	9000
skype	23739585	172778410
	13017940882	44589623764
	0	0
	3948000	1881000
imap	69793047	87941663
	4704034122	65548233051
	0	0
	162000	5527000
notes	370424960	2651705
	238136801236	774880651
	0	0
	4693000	448000
ftp	18165095	634433
	1372210386	911782424

2.3 Manejo de la Congestión

La congestión puede interpretarse como un fenómeno cuando la red maneja más tráfico del que puede soportar . La congestión en la red puede presentarse por diversas causas, provocando que la red presente problemas de ancho de banda, delay, jitter y especialmente perdida de paquetes. Las causas que se presentan con mayor frecuencia son:

- Ancho de banda muy limitado.
- Insuficiente performance en los equipos de los nodos.
- La velocidad de la interfaz de entrada es mayor a la interfaz de salida.
- Muchas interfaces de entrada convergen en una sola interfaz de salida.
- Desbordamiento de la memoria de entrada o de salida

El manejo de la congestión se puede realizar utilizando técnicas de control de congestión, las cuales, controlan la inyección del tráfico a la red manteniendo una distribución equilibrada

del ancho de banda para aquellas aplicaciones que exceden el ancho de banda. Cuando la congestión de red se presenta permanentemente dentro de la red, es necesario realizar un incremento del ancho de banda, mientras que, cuando la congestión de la red se presente temporalmente dentro de la red, es recomendable aplicar las técnicas de control de congestión conocidas como Queuing.

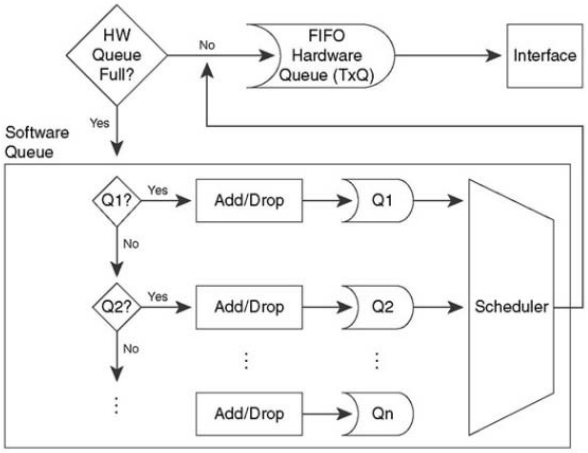
2.3.1 Introducción a Queuing

Queuing o encolamiento son técnicas de control de congestión que permiten entre otras cosas almacenar el tráfico en la interfaz de salida o entrada hasta que pueda ser procesado y enviado. La perdida de paquetes o la eliminación indiscriminada de los paquetes representa el mayor problema al no utilizar técnicas de control de congestión. Una de las interfaces, sea de entrada o salida puede manejar colas de hardware y colas de software. El algoritmo de congestión que se utilice permitira que un paquete, dependiendo del orden en que llegue, este podrá ser enviado.

Los componentes de la cola de hardware y software dependen una de la otra. En caso de que la cola de hardware no presente congestión, los paquetes serán procesados y enviados por la cola de hardware sin basarse en algoritmos de colas de software. En el caso de que la cola de hardware presente congestión, los paquetes serán procesados y enviados por la cola de hardware pero basandose en los algoritmos de colas de software.

La figura 2.31 presenta los componetes de la cola de Hardware y Software.

Figura 2. 33 (What-When-How) Colas de HW y SW



2.3.2 Algoritmos de Queuing

2.3.2.1 FIFO

Es el algoritmo de colas que se presenta en las interfaces de manera predeterminada y no requiere de ninguna configuración. Firt in, Firt out, primer paquete en ingresar es el primer paquete en salir, sin brindar ningún tipo de prioridad sobre los paquetes.

FIFO no es recomendado en las implementaciones de calidad de servicio ya que no permite priorizar los paquetes sobre otros y especialmente porque presenta limitaciones en sus bufers al momento de presentarse la congestión, almacenando los paquetes y enviándolos cuando tenga posibilidades respentando el orden de ingreso.

Al no poder priorizar los paquetes, los aplicativos más agresivos y de mayor generación de tráfico pueden generar perdidas o retardo en los paquetes más importantes como la voz o de criticidad alta dentro de una organización.

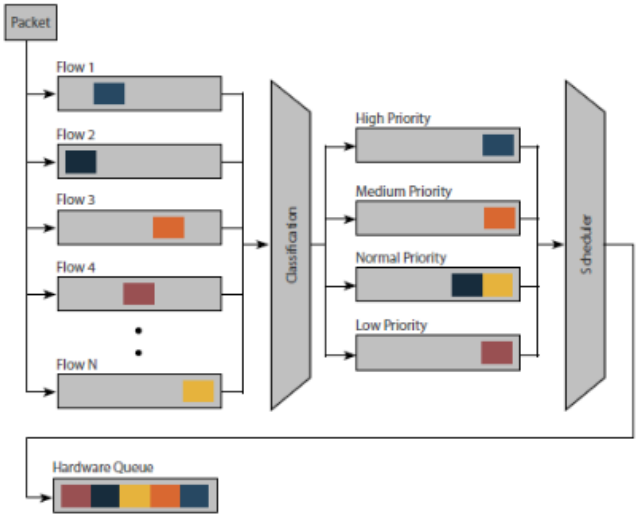
2.3.2.2 PQ

Es el algoritmo de colas que permite clasificar el tráfico dentro de cuatro colas: Prioridad Alta, Prioridad Media, Prioridad Normal y Prioridad Baja mediante configuración. Priority Queuing permite dar mayor prioridad a los paquetes más importantes, presentando un funcionamiento muy particular al dar mayor importancia a la cola de alta prioridad.

Cuando la cola de alta prioridad tiene paquetes, el programador PQ reenvía los paquetes solo de la cola de alta prioridad. Si la cola de alta prioridad está vacía, se procesa un paquete de la cola de prioridad media. Si están vacías las colas de prioridad alta y media, se procesa un paquete de la cola de prioridad normal, y si la cola de alto, medio y de prioridad normal están vacías, se procesa un paquete de la cola de baja prioridad. Es importante tener en cuenta que mientras los paquetes sigan entrando a la cola de alta prioridad, ninguna de las otras colas serán atendidas. Este comportamiento puede traer inconvenientes de descarte de paquetes dentro de las colas de prioridad normal o baja, ya que nunca serán atendidas mientras las colas de prioridad alta y media esten vacias. Si las colas no son configuradas adecuadamente, los paquetes que ingresan son asignados directamente a la cola de prioridad normal.

Los paquetes son asignados a cualquiera de las 4 tipos de colas tomando en cuenta su protocolo, dirección origen, dirección destino, tamaño, puerto de origen o puerto de destino. PQ es recomendable usarlo en interfaces que manejan poco ancho de banda y se requiere de priorización de tráfico.

Figura 2. 34 (Ciscoblog.ru) Colas de Prioridad PQ



2.3.2.3 RR

Es el algoritmo de colas que permite asignar paquetes a distintas colas sin manejar prioridad entre ellas. El ancho de banda es dividido por igual para cada una de las colas creadas, garantizando el ancho de banda por cada cola. Round Robin procesa un paquete de la primera cola y continua procesando un paquete de la siguiente cola y así sucesivamente hasta llegar a la última cola y repite el mismo proceso comenzando desde la primera cola.

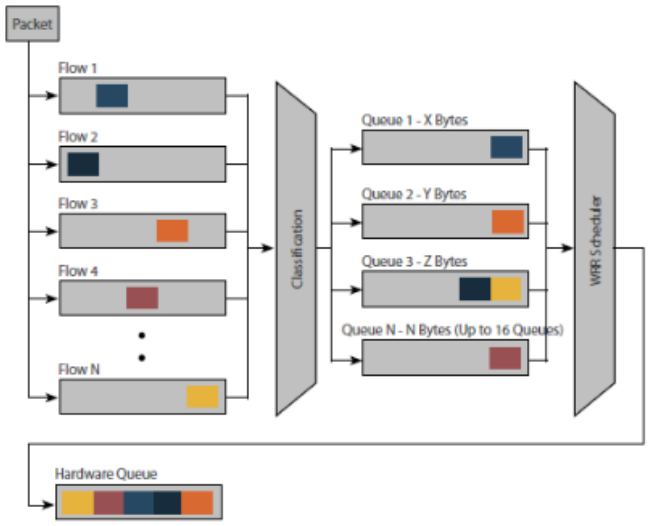
RR no permite manejar prioridad en el tráfico y cualquier tráfico importante puede ser destinado a cualquiera de las colas creadas.

2.3.2.4 WRR

Representa una mejora del algoritmo RR descrito anteriormente. Básicamente este algoritmo permite asignar paquetes a distintas colas pero manejando una prioridad basada en el peso. Entre mayor sea el peso de la cola, mayor prioridad tiene la cola y el ancho de banda es asignado

dependiendo del peso de la cola, garantizando mayor ancho de banda a los aplicativos de mayor prioridad, que difiere al ancho de banda de las otras colas. El proceso de atención es similar que Round Robin, en donde se procesa un paquete de la primera cola y continua procesando un paquete de la siguiente cola y así sucesivamente hasta llegar a la última cola y repite el mismo proceso comenzando desde la primera cola.

Figura 2. 35 (Ciscoblog.ru) Colas de WRR



2.3.3 Mecanismos de Encolamiento

2.3.3.1 WFQ (Weighted Fair Queuing)

Es el mecanismo más simple de los equipos router espacialmente CISCO, él cual permite dividir el tráfico en flujos, asignar ancho de banda equitativo para todos los flujos y asegurar el ancho de banda a los flujos más importantes.

WFQ ordena el tráfico en flujos, utilizando una combinación de parámetros. Por ejemplo, para una conversación TCP/IP, se utiliza como filtro el protocolo IP, dirección IP fuente,

dirección IP destino, puerto de origen, etc. Una vez distinguidos estos flujos, el enrutador determina cuáles son de uso intensivo o sensibles al retardo, priorizándolos y asegurando que los flujos de alto volumen sean empujados al final de la cola, y los volúmenes bajos, sensibles al retardo, sean empujados al principio de la cola. WFQ es apropiado en situaciones donde se desea proveer un tiempo de respuesta consistente ante usuarios que generen altas y bajas cargas en la red, ya que WFQ se adapta a las condiciones cambiantes del tráfico en ésta. Sin embargo, la carga que significa para el procesador en los equipos de enrutamiento, hace de esta metodología poco escalable, al requerir recursos adicionales en la clasificación y manipulación dinámica de las colas. (Bravo, 2011)

Las ventajes de WFQ son:

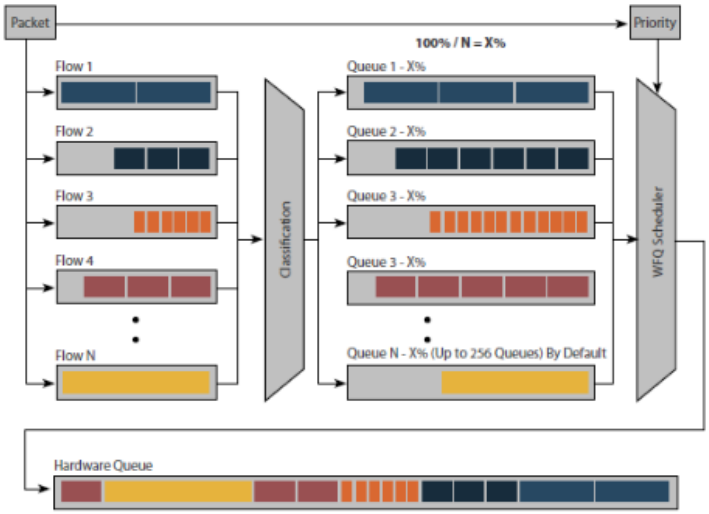
- Configuración simple y no requiere de ninguna clasificación explícita.
- Garantiza rendimiento a todos los flujos.
- Desecha paquetes de los flujos más agresivos y proporciona un servicio más rápido a los flujos no agresivos.
- Garantiza una entrega equitativa del ancho de banda
- Estándar compatible con la mayoría de plataformas Cisco

Las desventajas de WFQ son:

- No permite realizar la configuración manual de clases, y no permite asignar ancho de banda con valores fijos.
- No es un mecanismo escalable debido a que no puede mantener un numero alto de servicios en interfaces de alta velocidad.

- Funciona en interfaces iguales o menores a un E1

Figura 2. 36 (Ciscoblog.ru) WFQ



Los comandos utilizados para modificar o activar los parámetros de WFQ son lo siguientes:

❖ *Router(config-if)#* **fair-queue** *[congestive-discard-threshold [dynamic-queues [reservable-queues]]]*

congestive-discard-threshold: Es el número máximo de paquetes que una cola WFQ puede manejar (un nuevo valor debe ser potencia de 2 en el rango de 16 a 4096; el defaultes 64)

dynamic-queues: Es el número máximo de colas WFQ que pueden crearse (posibles valores:16, 32, 64, 128, 256, 512, 1024, 2048 y 4096; el default es256)

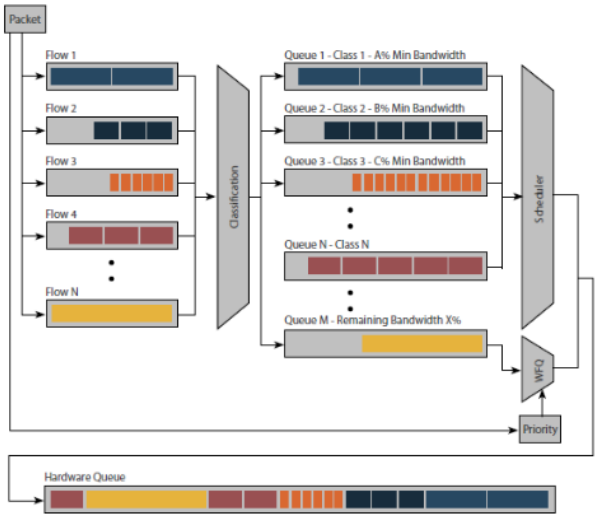
reservable-queues: Es el número de colas reservadas para servicios especiales

2.3.3.2 CBWFQ (Class Based Weighted Fair Queuing)

CBWFQ está basada en colas por espera equitativa ponderada basadas en clases, fue desarrollada para evitar limitantes y extender la funcionalidad del algoritmo WFQ, permitiendo

la incorporación de clases definidas por el usuario, que permiten un mayor control sobre las colas de tráfico y asignación de ancho de banda por parte del usuario. (Bravo, 2011)

Figura 2. 37 (Ciscoblog.ru) CBWFQ



CBWFQ utiliza class map para realizar la clasificación, dependiendo de la versión del IOS del dispositivo. En cuanto a la planificación y asignación de ancho de banda se basa en el peso que es asignado a cada cola por parte del usuario, igualmente calculado por el IOS del dispositivo. El ancho de banda puede ser asignado de 3 formas:

- *Ancho de banda en kbps:* Asignación de ancho de banda en velocidad de bits.
- *Ancho de banda en porcentaje:* Asignación de un porcentaje de ancho de banda disponible en la interfaz.
- *Ancho de banda restante en porcentaje:* Asignación de un porcentaje de ancho de banda disponible que no ha sido asignado a otras clases.

De la totalidad de porcentaje de ancho de banda de una interface, unicamente el 75% esta destinado para reservas, conocido como max-reserved-bandwith, mientras que el 25% esta

destinado para otro tipo de tráfico. La configuración mantenida en max-reserved-bandwith puede ser modificada pero no es recomendable hacerlo.

Las ventajes de CBWFQ son:

- Permite la creación de clases de tráfico definidas por el usuario. Estas clases se pueden definir usando mapas de clase MQC.
- Permite reserva y asignación de ancho de banda para cada clase de tráfico basado en preferencias y políticas del usuario.
- Permite definir hasta 64 clases de tráfico basadas en las políticas del usuario y aplicaciones de red existentes, en lugar de depender de la creación automática y dinámica de las colas basada en el flujo como WFQ, proporcionando escalabilidad.

Las desventajas de WFQ son:

- No ofrece una cola adecuada para aplicaciones en tiempo real como voz o video y sobre otras aplicaciones de IP

Para realizar la configuración de CBWFQ es necesario crear class map que contienen las distintas clases de tráficos. Según lo revisado en el capitulo 2.1.4, se utiliza el Método de Implementación MQC. A partir de la clase creada, se configuran los parámetros de ancho de banda según el criterio que se desea:

- *Router(config)#* **policy-map** *policy-name*
- *Router(config-pmap)#* **class-map** *class-name*

- *Router(config-pmap-c)#* **bandwidth** *{bandwidth-kbps* | **percent** *percentage* | **remaining percent** *percentage}* (bandwidth-kbps: Ancho de banda en bits y percentage: Valor en porcentaje segun el porentaje de reserva de la interfaz).

Es posible configurar parámetros adicionales que definen el numero máximo de paquetes que una cola puede contener y el tratamiento para el tráfico por defecto.

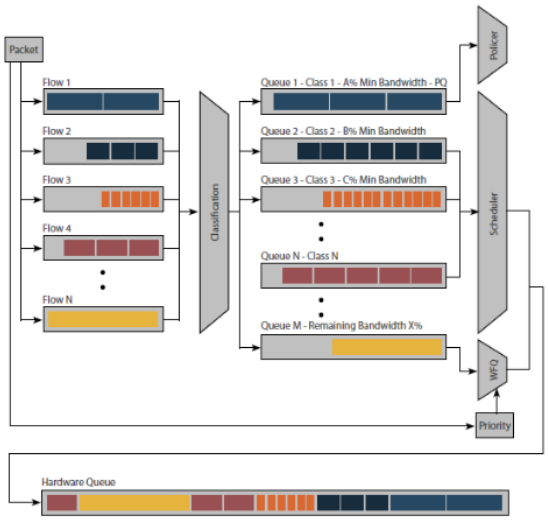
- *Router(config-pmap-c)#* **queue-limit**
- *Router(config-pmap-c)#* **fair-queue**

2.3.3.3 LLQ (Low Latency Queuing)

LLQ es el método de encolamiento recomendado para Voz sobre IP (VoIP) y telefonía IP y, además también trabajará apropiadamente con videoconferencias. LLQ consta de colas de prioridad estrictas (strict-priority queue), basadas en clases de tráficos, en conjunto con una cola de prioridad, la cual tiene preferencia absoluta sobre las otras colas ya que este tipo de tráfico es susceptible al retardo y al descarte de paquetes por ser aplicaciones que trabajan en tiempo real. (Bravo, 2011)

La cola de prioridad estricta permite ofrecer garantías de baja latencia y ancho de banda mínimo para el tráfico mas sensible, pero también puede presentar problemas de desecho de paquetes ya que estas colas deben ser configuradas con un límite de ancho de banda reservado.

Figura 2. 38 (Ciscoblog.ru) LLQ



Las ventajes de LLQ son:

- Ofrece las mismas ventajas de CBWFQ.
- Permite la creación de una o más colas de prioridad estricta con garantías de ancho de banda para el tráfico sensible retardo y jitter.

Para realizar la configuración de LLQ es necesario crear class map que contienen las distintas clases de tráficos. Según lo revisado en el capitulo 2.1.4, se utiliza el Método de Implementación MQC. A partir de la clase creada, se asigna la cola de prioridad estricta garantizando el ancho de banda.

- *Router(config)#* ***policy-map*** *policy-name*
- *Router(config-pmap)#* ***class-map*** *class-name*
- *Router(config-pmap-c)#* **priority** *{bandwidth-kbps* | **percent** *percentage} [burst]* (bandwidth-kbps: Ancho de banda en bits y percentage: Valor en porcentaje segun el porentaje de reserva de la interfaz)

CAPÍTULO 3

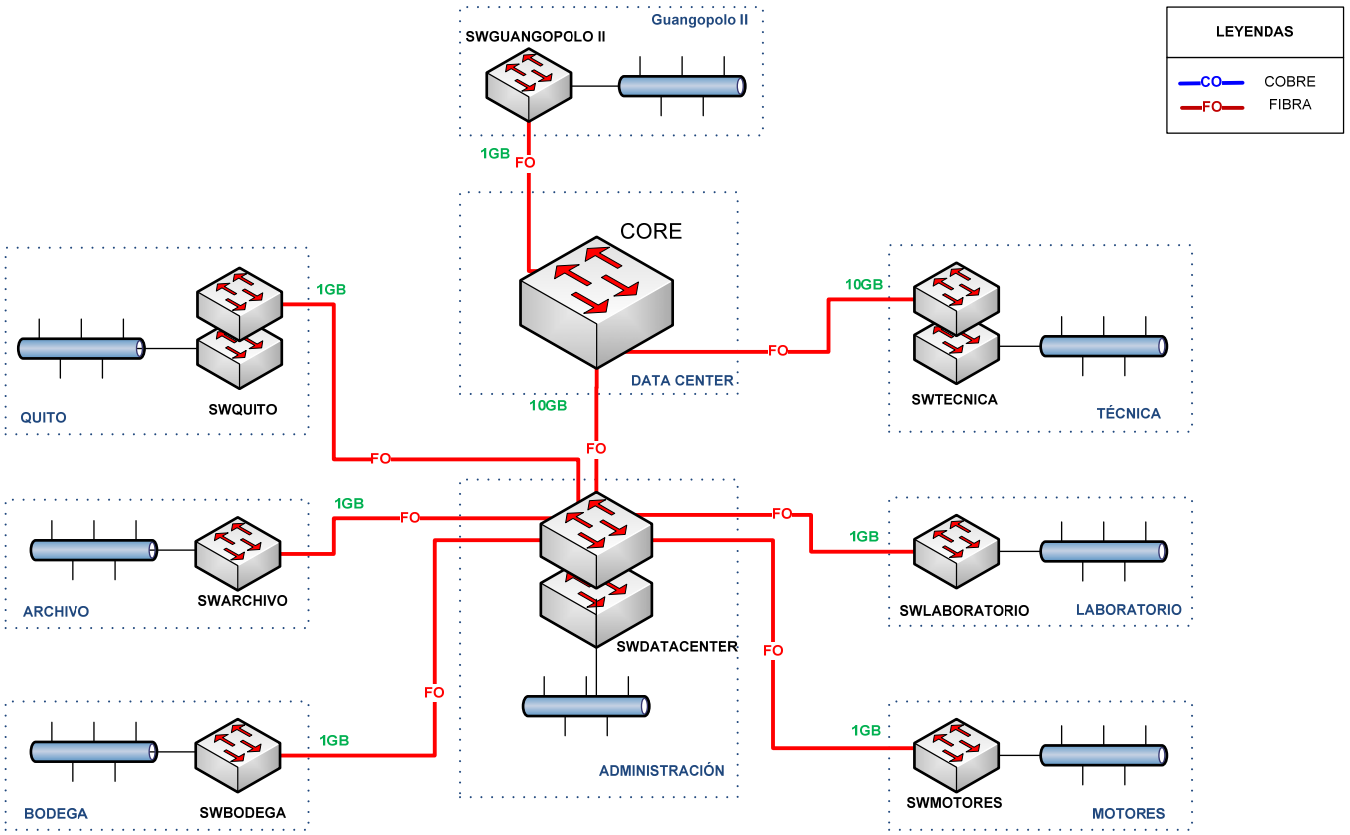
INFRAESTRUCTURA DE RED TERMOPICHINCHA

3.1 Topología de Red Lógica

3.1.1 LAN

La topología de red LAN utilizada actualmente es de tipo estrella, la cual enlaza 7 nodos en diferente ubicación mediante canales de fibra óptica de tipo multimodo y monomodo, que convergen en otro nodo ubicado en el Data Center.

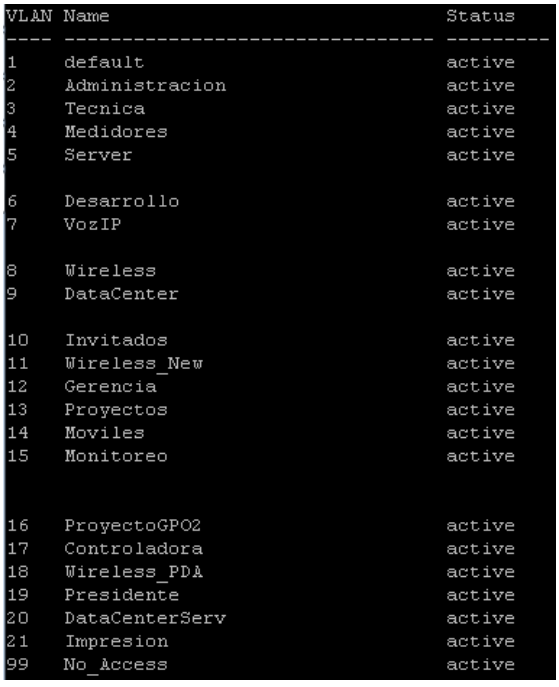
Figura 3. 1 Distribución Infraestructura de red LAN



La distribución lógica de la red LAN de la Unidad de Negocios Termopichincha se detalla en la Figura 3.1. Un switch de CORE situado en el centro de la topología en estrella, ubicado en el Data Center, desde este se distribuye 3 enlaces hacia 3 switch de acceso, 2 enlaces de 10 GB hacia el área Técnica y Data Center, y 1 enlace de 1 GB hacia Guangopolo II. Adicionalmente se distribuye 4 enlaces hacia 5 switch de acceso de 1 GB cada uno hacia las áreas de Quito, Archivo, Bodega, Motores y Laboratorio.

Se mantiene una configuración de VTP en el switch de CORE, la cual es replicada en cada uno de los switchs de comunicación de los nodos, permitiendo que las configuraciones de vlans se la realice de manera centralizada en el switch de core. Por el momento se manejan 22 vlans, como se muestra en la figura 3.2, destinadas para diferentes requerimientos de la organización y adicionalmente destinadas para cada nodo de la topología, con el fin de evitar inconvenientes como broadcast y mantener una mejor administración de la red.

Figura 3. 2 VLANS switch CORE



VLAN	Name	Status
1	default	active
2	Administracion	active
3	Tecnica	active
4	Medidores	active
5	Server	active
6	Desarrollo	active
7	VozIP	active
8	Wireless	active
9	DataCenter	active
10	Invitados	active
11	Wireless_New	active
12	Gerencia	active
13	Proyectos	active
14	Moviles	active
15	Monitoreo	active
16	ProyectoGPO2	active
17	Controladora	active
18	Wireless_PDA	active
19	Presidente	active
20	DataCenterServ	active
21	Impresion	active
99	No_Access	active

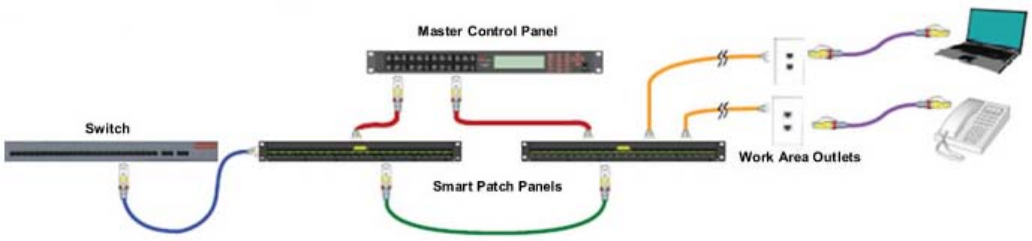
3.1.1.1 Cableado Estructurado

La Unidad de Negocios Termopichincha mantiene un cableado estructurado categoría 6A de marca Siemon. Se tiene alrededor de 350 puntos de red con dicha categoría que va desde los paneles donde se ubica el switch de acceso hasta la estación de trabajo.

Una de las características principales del cableado estructurado es que maneja una tecnología llamada "Cableado Inteligente MapIT G2" el cual ofrece una visibilidad completa y total control de la capa física de la red.

La distribución lógica del MapIT G2 de la Unidad de Negocios Termopichincha se detalla en la Figura 3.3, en la cual, desde los switchs de acceso se realiza una conexión hacia el panel conocido como SPP (Smart Patch Panel), luego se realiza una conexión en espejo de los mismos puertos del SPP hacia otro SPP, el cual maneja la distribución de los puntos de red hacia el usuario final. Los SPP permiten realizar el monitoreo de cada uno de los puertos, pero estos deben estar conectados hacia un panel de control principal llamado MCP (Master Control Panel). En forma general, El software que monitorea el cableado estructurado mantiene conexión permanente hacia los SPP y MCP.

Figura 3. 3 Distribución Lógica de MapIT

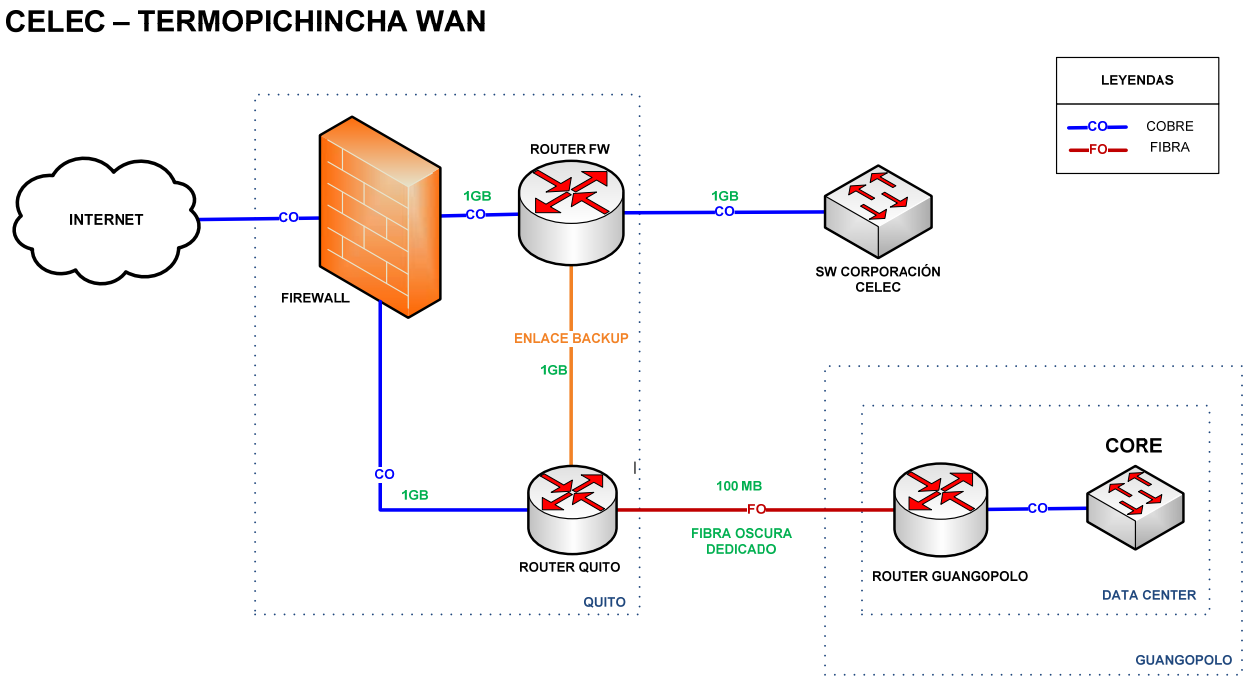


3.1.2 WAN

La topología de red WAN utilizada actualmente comprende dos nodos principales conectados mediante un canal oscuro de fibra óptica dedicada. Todo el tráfico de red dirigida hacia el Internet pasa por el enlace WAN hasta llegar al equipo perimetral, el cual tiene la salida hacia el internet. Todo el tráfico de red dirigido hacia la Corporación pasa por el enlace WAN hasta llegar al equipo perimetral, el cual dirige el tráfico hacia el router que da la cara hacia la Corporación CELEC.

Por la importancia de mantener una comunicación continua con la Corporación CELEC, se tiene configurado un enlace WAN de backup que re direcciona el tráfico de red hacia el router que da la cara a la Corporación sin pasar por el equipo perimetral en el caso de fallas.

Figura 3. 4 Distribución Infraestructura de red WAN



La distribución lógica de la red WAN de la Unidad de Negocios Termopichincha se detalla en la Figura 3.4. Dentro del Data Center ubicado en la Central Guangopolo se encuentra el

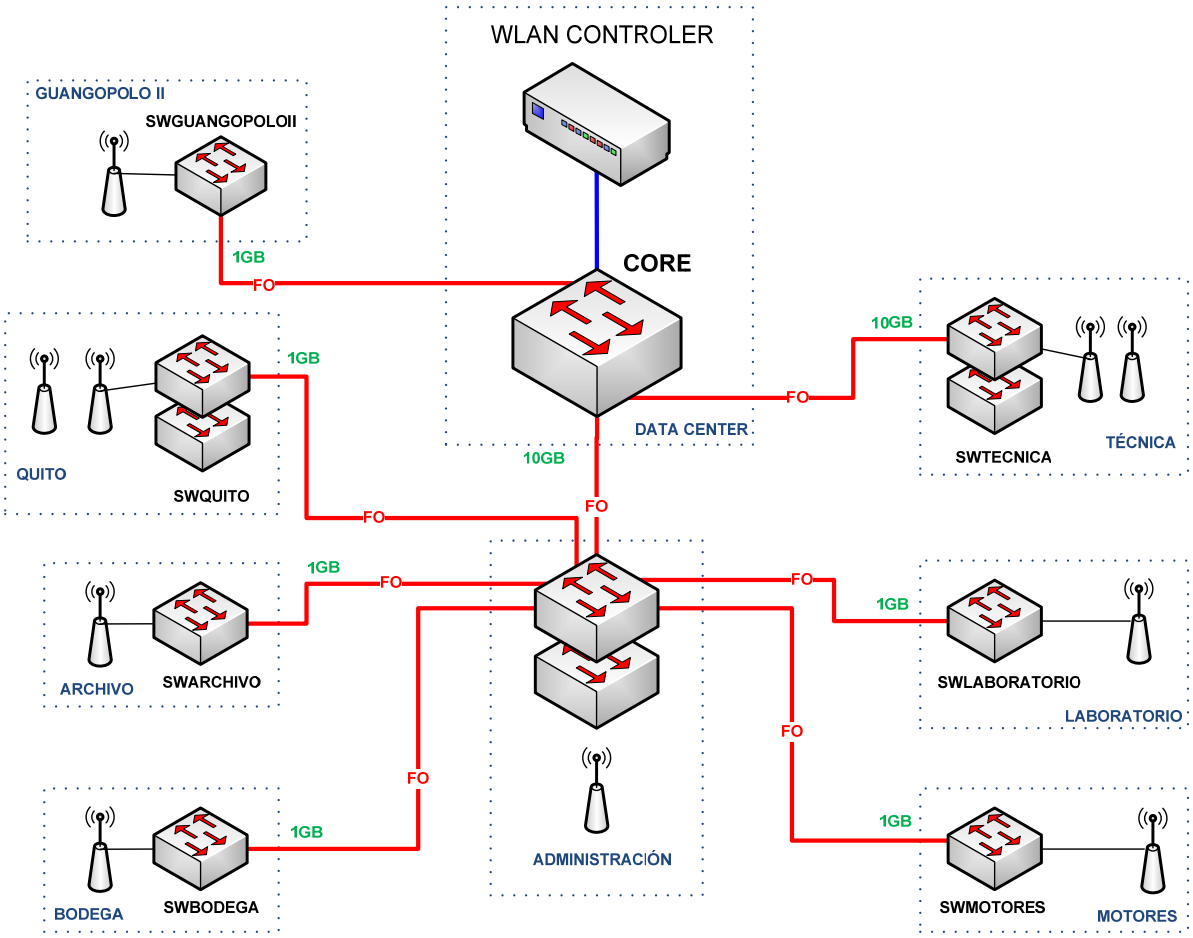
switch de CORE el cual envía todo el tráfico externo (internet, centrales remotas o corporativo) hacia el Router Guangopolo, desde este se estable una comunicación directa de 100MB mediante fibra de aproximadamente 30 km hacia el Router Quito. Dentro de las oficinas de Quito se encuentran ubicados tanto el Firewall, el Routerfw y el Router Quito. Entre el Router Quito y el Routerfw se encuentra levantado un enlace de backup en el caso de daños del equipo Firewall. Desde el Routerfw se establece una comunicación directa hacia el switch Corporativo.

3.1.3 Wireless

Dentro de la topología de red LAN se mantiene integrada la red wireless, la cual está conformada por un controlador de red inalámbrico que centraliza la comunicación y configuraciones de las redes wireless en cada uno de los 7 nodos. Dentro del dominio VTP se maneja vlans dedicadas para las redes wireless.

La distribución lógica de la red LAN - Wireless de la Unidad de Negocios Termopichincha se detalla en la Figura 3.5. Un switch de CORE situado en el centro de la topología en estrella, ubicado en el Data Center, a este se conecta directamente la controladora LAN y se distribuye 3 enlaces hacia 3 switch de acceso, 2 enlaces de 10 GB hacia el área Técnica y Data Center, y 1 enlace de 1 GB hacia Guangopolo II. Adicionalmente se distribuye 4 enlaces hacia 5 switch de acceso de 1 GB cada uno hacia las áreas de Quito, Archivo, Bodega, Motores y Laboratorio. En cada uno de los sitios mencionados se encuentra un access point que funciona de manera LWAPP (Lightweight Mode), esto quiere decir que dependen de la controladora principal, la cual distribuye las configuraciones y cambios a todos los access point que están asociados.

Figura 3. 5 Distribución Infraestructura de red LAN Wireless



3.2 Topología de Red Física

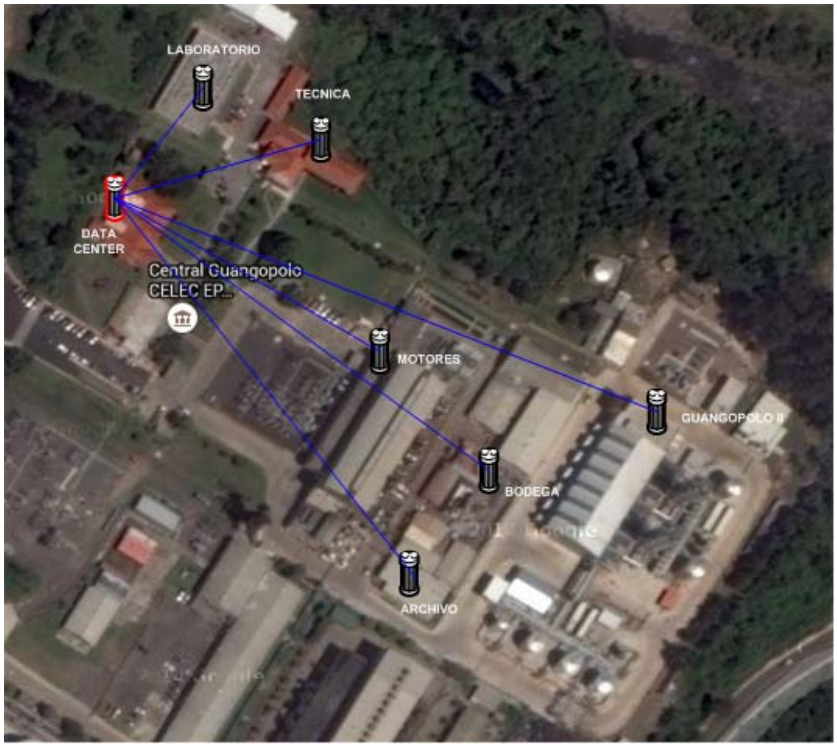
3.2.1 LAN

La topología de red física LAN está conformada por dos ubicaciones geográficas importantes que son: Quito y Guangopolo - Valle de los Chillos. En cada uno de las ubicaciones se encuentran repartidos todos los departamentos Administrativos y Técnicos de la organización.

En la ubicación de Guangopolo existen actualmente 7 nodos ubicados en diferentes sitios e interconectados mediante canales de fibra óptica que convergen en uno de los nodos ubicado

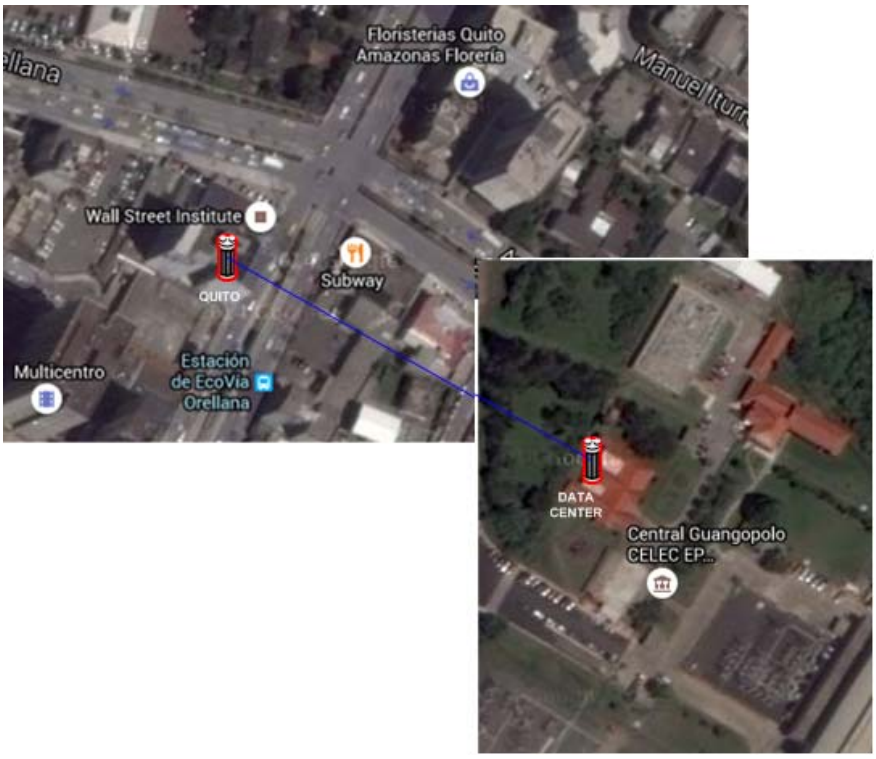
dentro del data center. En cada nodo se encuentra colocado un switch administrable de capa 2 y un ODF de fibra óptica.

Figura 3. 6 Topología de red LAN física de Guangopolo



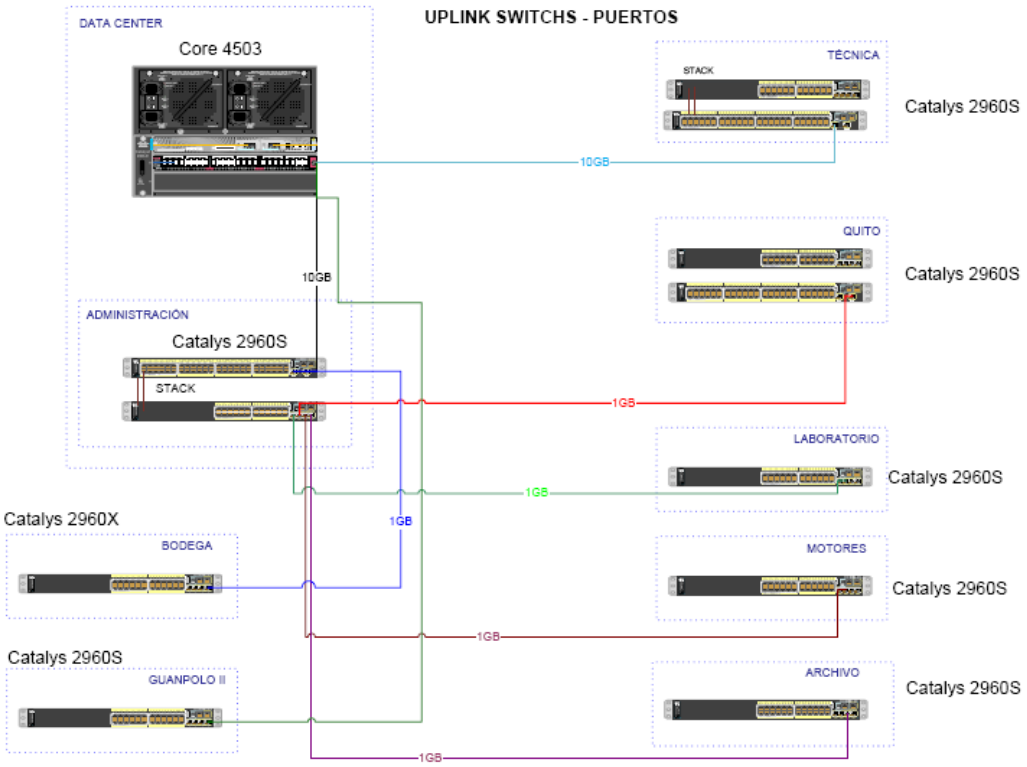
En la ubicación de Quito existe actualmente 1 nodo en la Av. Orellana y 6 de Diciembre dentro del edificio de Transelectric. Este nodo tiene una conexión LAN directa hacia el data center ubicada en Guangopolo, cubriendo alrededor de 30 km de distancia entre ambos puntos. En este nodo se encuentra colocado un switch administrable de capa 2 y un ODF de fibra óptica.

Figura 3. 7 Topología de red LAN física de Quito



Los equipos switch de cada nodo se encuentran conectados mediantes módulos de fibra de 10 GB o 1 GB. El switch ubicado en el data center es un switch de CORE de capa 3 y el concentrador de las conexiones de fibra de cada nodo.

Figura 3. 8 Uplink equipos switch



Como se puede observar en la figura 3.8, la trayectoria de fibra óptica que va desde el Data Center hasta el nodo de Laboratorio tiene una distancia de 40 metros y es de tipo multimodo utilizando un modulo SFP de 1 GB , desde el Data Center hasta el nodo de la Técnica tiene una distancia de 80 metros y es de tipo multimodo utilizando un modulo SFP de 10 GB, desde el Data Center hasta el nodo de Quito tiene una distancia de 30 kilómetros y es de tipo monomodo utilizando un modulo SFP de 1 GB, desde el Data Center hasta el nodo de Motores tiene una distancia de 85 metros y es de tipo multimodo utilizando un modulo SFP de 1 GB, desde el Data Center hasta el nodo de Archivo tiene una distancia de 150 metros y es de tipo monomodo utilizando un modulo SFP de 1 GB, desde el Data Center hasta el nodo de Guangopolo II tiene una distancia de 200 metros y es de tipo monomodo utilizando un modulo SFP de 1 GB y desde

el Data Center hasta el nodo de Bodega tiene una distancia de 170 metros y es de tipo monomodo utilizando un modulo SFP de 1 GB.

3.2.2 WAN

La topología de red física WAN está conformada por dos ubicaciones geográficas importantes que son: Quito y Guangopolo - Valle de los Chillos.

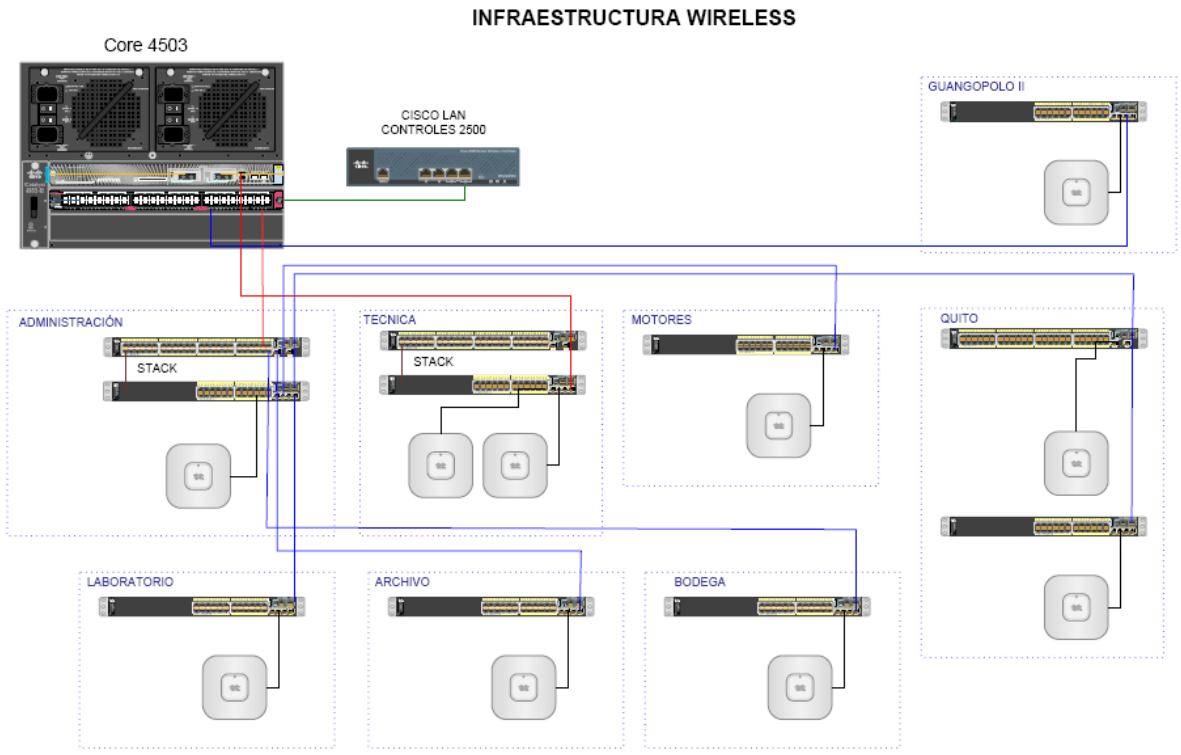
En la ubicación de Guangopolo se encuentra colocado un router a continuación del switch de core, mientras que en la ubicación de Quito se encuentra colocado 2 routers. El primer router maneja la WAN hacia Guangopolo, mientras que el segundo router maneja la WAN hacia la corporación.

El canal de fibra óptica que utiliza el enlace WAN entre ambas ubicaciones cubre una distancia aproximada de 30 km, monomodo y atraviesa en su trayectoria por 6 nodos. El primer nodo cubre la trayectoria entre la Central Guangopolo y La Central Gualberto Hernández de la EEQ, el segundo nodo cubre la trayectoria entre La Central Gualberto Hernández y La Hidráulica, el tercer nodo cubre la trayectoria entre La Hidráulica y la Estación Centro Sur, el cuarto nodo cubre la trayectoria entre la Estación Centro Sur y Central Vicentina, el quinto nodo cubre la trayectoria entre la Central Vicentina y la Subestación Vicentina de Transelectric y el sexto nodo cubre la trayectoria entre la Subestación Vicentina de Transelectric y el Edifico de Transelectric (Av. Orellana y 6 de Diciembre). Es importante mencionar que la fibra óptica que utiliza el enlace WAN desde el nodo Central Guangopolo hasta Subestación Vicentina de Transelectric es rentada a la Empresa Eléctrica Quito.

3.2.3 Wireless

Debido a que la a topología de red física LAN está conformada por dos ubicaciones geográficas importantes que son: Quito y Guangopolo (Valle de los Chillos), la red wireless se encuentra distribuida en las mismas ubicaciones como se detalla en la Figura 3.9. Cada access point se encuentra ubicado en cada uno de los sitios y mediante el canal de comunicaciones se asocian a la controladora LAN. Es importante resaltar que para colocar un access point en la ubicación de Quito que esté asociada a la controladora LAN, se tuvo que utilizar el canal LAN de 30 km desde el Data Center.

Figura 3. 9 Topología física de la red LAN Wireless



3.3 Equipamiento de Comunicaciones

La Unidad de Negocios de Termopichincha cuenta con un equipamiento de comunicaciones de la línea CISCO en toda su infraestructura LAN, WAN y Wireless. Al mantener la línea del

propietario CISCO se ha conseguido aprovechar todos los beneficios que ésta brinda dentro de la infraestructura de red como configuraciones, compatibilidad, protocolos propietarios, enrutamientos, switching, etc.

3.3.1 Equipamiento LAN

La Tabla 3.1 describe los equipos de comunicación de los diferentes nodos ubicados en Guangopolo, haciendo referencia a la figura 3.1, 3.5, 3.8 y 3.9.

Tabla 3. 1 Equipos de comunicaciones LAN nodo Guangopolo

NODO	EQUIPO	MARCA	MODELO	IOS	ESTADO
DATA CENTER (ADMINISTRACIÓN)	Catalyst 4500 L3 Switch	Cisco	WS-C4503-E	CAT 4500e-LANBASE-M, Versión 12.2(53) SG2	ACTIVO
	Catalyst 2960 L2 Switch	Cisco	WS-C2960S-48FPD-L	C2960S-UNIVERSALK9-M, Version 12.2 (55) SE5	ACTIVO
	Catalyst 2960 L2 Switch	Cisco	WS-C2960S-24PS-L	C2960S-UNIVERSALK9-M, Version 12.2 (55) SE5	ACTIVO
	Cisco 2500 Series Wireless Controller	Cisco	AIR-CT2504-K9		ACTIVO
	Cisco Wireless Access Point	Cisco	AIR-CAP3501I-A-K9	AP3G1-K9W8-M, Version 12.4(23c)JA3	ACTIVO
LABORATORIO	Catalyst 2960 L2 Switch	Cisco	WS-C2960S-24PS-L	C2960S-UNIVERSALK9-M, Version 12.2 (55) SE5	ACTIVO
	Cisco Wireless Access Point	Cisco	AIR-CAP3501I-A-K9	AP3G1-K9W8-M, Version 12.4(23c)JA3	ACTIVO
	Catalyst 2960 L2 Switch	Cisco	WS-C2960S-48FPD-L	C2960S-UNIVERSALK9-M, Version 12.2 (55) SE5	ACTIVO

TECNICA	Catalyst 2960 L2 Switch	Cisco	WS-C2960S-24PS-L	C2960S-UNIVERSALK9-M, Version 12.2 (55) SE5	**ACTIVO**
	Cisco Wireless Access Point	Cisco	AIR-CAP3501I-A-K9	AP3G1-K9W8-M, Version 12.4(23c)JA3	**ACTIVO**
	Cisco Wireless Access Point	Cisco	AIR-CAP3501I-A-K9	AP3G1-K9W8-M, Version 12.4(23c)JA3	**ACTIVO**
MOTORES	Catalyst 2960 L2 Switch	Cisco	WS-C2960S-24PS-L	C2960S-UNIVERSALK9-M, Version 12.2 (55) SE5	**ACTIVO**
	Cisco Wireless Access Point	Cisco	AIR-LAP1141N-A-K9	WLC2504 Version 7.0.220.0	**ACTIVO**
GUANGOPOLO II	Catalyst 2960 L2 Switch	Cisco	WS-C2960S-24PS-L	C2960S-UNIVERSALK9-M, Version 12.2 (55) SE5	**ACTIVO**
	Cisco Wireless Access Point	Cisco	AIR-LAP1141N-A-K9	Version 12.4(23c)JA3	**ACTIVO**
ARCHIVO	Catalyst 2960 L2 Switch	Cisco	WS-C2960S-24PS-L	C2960S-UNIVERSALK9-M, Version 12.2 (55) SE5	**ACTIVO**
	Cisco Wireless Access Point	Cisco	AIR-LAP1141N-A-K9	Version 12.4(23c)JA3	**ACTIVO**
BODEGA	Catalyst 2960-X L2 Switch	Cisco	WS-C2960X-24PS-L	C2960X-UNIVERSALK9-M, Version 15.0(2a)EX5	**ACTIVO**
	Cisco Wireless Access Point	Cisco	AIR-CAP3501I-A-K9	AP3G1-K9W8-M, Version 12.4(23c)JA3	**ACTIVO**

La Tabla 3.2 describe los equipos de comunicación del nodo ubicado en Quito y haciendo referencia a la figura 3.1, 3.5, 3.8 y 3.9.

Tabla 3. 2 Equipos de comunicaciones LAN nodo Quito

NODO	EQUIPO	MARCA	MODELO	IOS	ESTADO
QUITO	Catalyst 2960 L2 Switch	Cisco	WS-C2960S-48LPS-L	C2960S-UNIVERSALK9-M, Version 12.2 (55) SE5	ACTIVO
	Catalyst 2960 L2 Switch	Cisco	WS-C2960S-24PS-L	C2960S-UNIVERSALK9-M, Version 12.2 (55) SE5	ACTIVO
	Cisco Wireless Access Point	Cisco	AIR-CAP3501I-A-K9	AP3G1-K9W8-M, Version 12.4(23c)JA3	ACTIVO
	Cisco Wireless Access Point	Cisco	AIR-LAP1141N-A-K9	Version 12.4(23c)JA3	ACTIVO

3.3.2 Equipamiento WAN

La Tabla 3.3 describe los equipos de comunicación de los diferentes nodos ubicados en Guangopolo, haciendo referencia a la figura 3.4.

Tabla 3. 3 Equipos de comunicaciones WAN nodo Guangopolo

NODO	EQUIPO	MARCA	MODELO	IOS	ESTADO
DATA CENTER	Cisco 1900 Series	Cisco	CISCO1921/K9	C1900-UNIVERSALK9-M, Version 15.1(4) M3	ACTIVO

La Tabla 3.4 describe los equipos de comunicación del nodo ubicado en Quito, haciendo referencia a la figura 3.4.

Tabla 3. 4 Equipos de comunicaciones WAN nodo Quito

NODO	EQUIPO	MARCA	MODELO	IOS	ESTADO
QUITO	Cisco 1900 Series	Cisco	CISCO1921/K9	C1900-UNIVERSALK9-M, Version 15.2(4) M6a	ACTIVO
	Cisco 1900 Series	Cisco	CISCO1921/K9	C1900-UNIVERSALK9-M, Version 15.2(4) M6a	ACTIVO

3.3.3 Características de los equipos de comunicación

A continuación se describen las características principales de los equipos de comunicación que conforman la red LAN, WAN y Wireless de la Unidad de Negocios Termopichincha y su aplicación en el tema de calidad de servicio (QoS).

3.3.3.1 Cisco Catalyst 2960

La serie Catalyst 2960 es ideal para brindar conectividad en entornos tradicionales de estaciones de trabajo tanto para Ethernet como para Gigabit Ethernet, lo que permite realizar operaciones simplificadas y automatizadas como políticas de seguridad para limitar el acceso a la red y mitigar las amenazas, implementar servicios de QoS para el tratamiento de prioridad del tráfico de voz y aplicaciones críticas (Cisco Systems, 2015). Las características más importantes son:

- Ancho de banda de switching de 100 Gbps
- MTU de 9198 bytes
- Gestión inteligente del tráfico.

- Mecanismos flexibles para el marcado, clasificación y programación.
- Rendimiento superior para el tráfico de datos, voz y video.
- Manejo de 4 colas de salida por puerto.

Figura 3. 10 Cisco Catalyst 2960s

La serie Catalyst 2960 configurado como un switch de acceso hacia los usuarios ha permitido mantener mayor velocidad hacia los servicios de red, como también, soportar configuraciones de dominio de VLANs administrados desde el switch de CORE, mejorando la administración de la infraestructura. Años atrás la Unidad de Negocios Termopichincha manejaba equipo de bajo rendimiento, impidiendo la expansión de la red y provocando saturaciones en los equipos. El cambio hacia esta serie ha permitido superar estos problemas y tener mayor beneficio en el tratamiento del tráfico. Adicionalmente es importante indicar que la característica mencionada anteriormente permite determinar que la serie 2960 es la adecuada para el flujo de trabajo que se desarrolla actualmente en la organización.

3.3.3.2 Cisco Router 1921

La serie Cisco 1900 de Servicios de Ruteo Integrado (ISRs) con un CPU multinúcleo, conmutación con Gigabit Ethernet, con Power over Ethernet y control de capacidades proporciona una base de tecnologías estable para adaptarse a los requisitos de la red y ofrecer una integración inteligente de comunicaciones unificadas, wireless, firewall, aceleración de

encriptación por hardware embebido, prevención de intrusos, servicios de seguridad avanzado y servicios de aplicación (Cisco Systems, 2015). Las características más importantes son:

- Implementación en entornos WAN de alta velocidad con servicios concurrentes habilitados arriba de 15MB.
- Procesadores multinúcleo de alto rendimiento.
- Interfaces modulares que permite mayor ancho de banda.
- Funciones de CBWFQ, WRED, NBAR.

Figura 3. 11 Cisco Router 1900 Series

A partir del crecimiento de la organización se presentaron inconvenientes de comunicación en los canales wan, el levantamiento de nuevos sitios remotos obligó a la Unidad de Negocios Termopichincha aplicar un cambio de diseño en la infraestructura, con la necesidad de brindar la mejor comunicación entre el sitio principal y los sitios remotos. La serie 1900 es una de las mejores alternativas planteadas para su implementación, ya que se pudo atacar varias necesidades y prevenir un crecimiento continuo. Estas necesidades fueron enfocadas en:

- Obtener el mejor rendimiento en un canal de fibra óptica (oscura) entre la Central Guangopolo y las Oficinas de Quito.
- Manejo de n enlaces wan hacia los sitios remotos.
- Manejo de enlaces de backup, mediante la utilización de servicios como IP SLAs.
- Mayores características de procesamiento, ruteo y ancho de banda.

Es importante indicar que el equipo actualmente ha cubierto con las necesidades antes mencionadas y posiblemente pueda soportar un mayor flujo de trabajo sin dificultad, pero los beneficios que presta permite determinar que la serie seleccionada es óptica y adecuada para soportar más servicios que podrían ser implementados en la Unidad de Negocios Termopichincha.

3.3.3.3 Cisco Wireless Access Point AIR-CAP3501I

La serie Cisco 3500 son los primeros puntos de acceso 802.11n en la industria capaces de crear una auto sanación y una auto optimización de la redes inalámbrica (Cisco Systems, 2015). Las características más importantes son:

- Tecnología ClearAir.
- Conectividad 802.11n.
- Integra antenas de 2.4 GHZ y 5 GHZ.
- Seguridad 802.11i, WPA2, WPA, 802.1X, Advanced Encryption Standards (AES) y Temporal Key Integrity Protocol (TKIP).
- Permite seleccionar el tráfico de red específico y priorizarlo.

Figura 3. 12 Cisco Access Point 3500

La serie Cisco 3500 ha permitido que los accesos a las redes inalámbricas sean administrados de mejor manera. Las capacidades de difusión de la señal han permitido poder cubrir grandes

áreas dentro de las oficinas de la Unidad de Negocios. Es importante tomar en cuenta que debido a las necesidades de la portabilidad de un computador que existe en la actualizada ha provocado que las capacidades y características del equipo no sean las adecuadas para soportar la cantidad de equipos portátiles que se manejan dentro de la Unidad. Es muy recomendable tomar en cuenta el mejoramiento de este equipo dentro del plan de cambio de infraestructura, ya sea: adquiriendo nuevo equipamiento o más puntos de acceso para equilibrar la carga. El problema está en el exceso de usuario, pero las funcionalidades que brinda son utilizadas en su totalidad.

3.3.3.4 Cisco Wireless Access Point AIR-LAP1141N

La serie Cisco 1140 es el punto de acceso de diseño simple y eficiencia de energía que ofrece por lo menos 6 veces el rendimiento de las redes 802.11 a/g. Sus características son menores al modelo mencionado anteriormente en cuanto a su cobertura.

Figura 3. 13 Cisco Access Point 1140

Como se mencionó anteriormente, los excesos de conexiones limitan el rendimiento del equipo. Debido a que es un modelo menor al anterior, este presenta con mayor frecuencia los problemas de saturación. Como medida preventiva, estos equipos han sido reinstalados en sitios en donde el acceso inalámbrico es menor y no requiere de una cobertura extensa. Adicionalmente estos equipos están siendo utilizados de manera Autonomous, sin la necesidad de un controlador LAN.

En cuanto a las características de QoS, da las mismas prestaciones que la serie Cisco 3500, en donde la priorización, clasificación y manejo de la congestión pueden ser aplicadas.

3.3.3.5 Cisco Wireless Control 2500

La serie Cisco Controladora 2500 son reguladores de nivel de entrada que proporcionan comunicación en tiempo real entre puntos de acceso Cisco Aironet para simplificar el despliegue, administración y operación de redes inalámbricas. Las características más importantes son:

- Soporta hasta 75 access point y 1000 clientes.
- Soporta hasta 1Gbps de throughput.
- Capacidades para la prevención de intrusos en redes inalámbricas (wIPS).
- Brinda calidad de servicio para voz y video.
- Aplicación de políticas de QoS.

Figura 3. 14 Cisco Wireless Control 2500

El Cisco Controladora 2500 ha permitido mantener una adecuada administración de todos los puntos de acceso vinculados y por sus capacidades, permitirá manejar un número mayor de puntos de acceso sin problema. Este modelo es adecuado para el ambiente actual, es estable y permite brindar mayores beneficios.

3.3.3.6 Cisco Catalyst 4503

La serie Cisco Catalyst 4500 son switchs de borde habilitados dentro de la red proporcionando alto desempeño móvil y seguridad para el usuario en capa 2 y 4. Permite un alto desempeño y velocidad en ruteo y conmutación de paquetes entre sus características principales. Adicionalmente permite la gestión inteligente del tráfico, mecanismos flexibles para el marcado, clasificación y programación y un rendimiento superior para el tráfico de datos, voz y video (Cisco Systems, 2015).

Figura 3. 15 Cisco Catalyst 4503

Con el objetivo de mantener un modelo jerárquico, compatibilidad con los switch de acceso y cubrir con las necesidades internas, se consideró al Cisco Catalyst 4503 como la mejor opción de implementación. El equipo se encuentra trabajando de manera CORE y distribución con enlaces internos de 10 GB y 1 GB entre los switchs de acceso. Al igual que los router 1921, es importante indicar que el equipo actualmente ha cubierto con las necesidades, sin presentar fallas en cuanto a su desempeño, pero es capaz de soportar un mayor flujo de trabajo sin dificultad.

A pesar de que el equipo puede ser equipado con más componente debido a su característica modular, actualmente el equipo mantiene los requerimientos básicos necesarios.

3.4 Servicios de Red

La Unidad de Negocios Termopichincha brinda dentro de su infraestructura interna servicios de red para el manejo transaccional, documental, industrial y comunicaciones. También existen servicios de red a nivel de Corporación, que mediante los enlaces de datos pueden ser consumidos por la Unidad de Negocios Termopichincha.

3.4.1 Sistema Financiero Integrado

El Sistema Financiero Integrado conocido como IFS es el sistema ERP manejado a nivel de Corporación.

IFS es una empresa reconocida globalmente como líder en el desarrollo y suministro de software corporativo para Planificación de Recursos Empresariales (ERP), Gestión de Activos Empresariales (EAM) y Gestión de Servicios Empresariales (ESM).

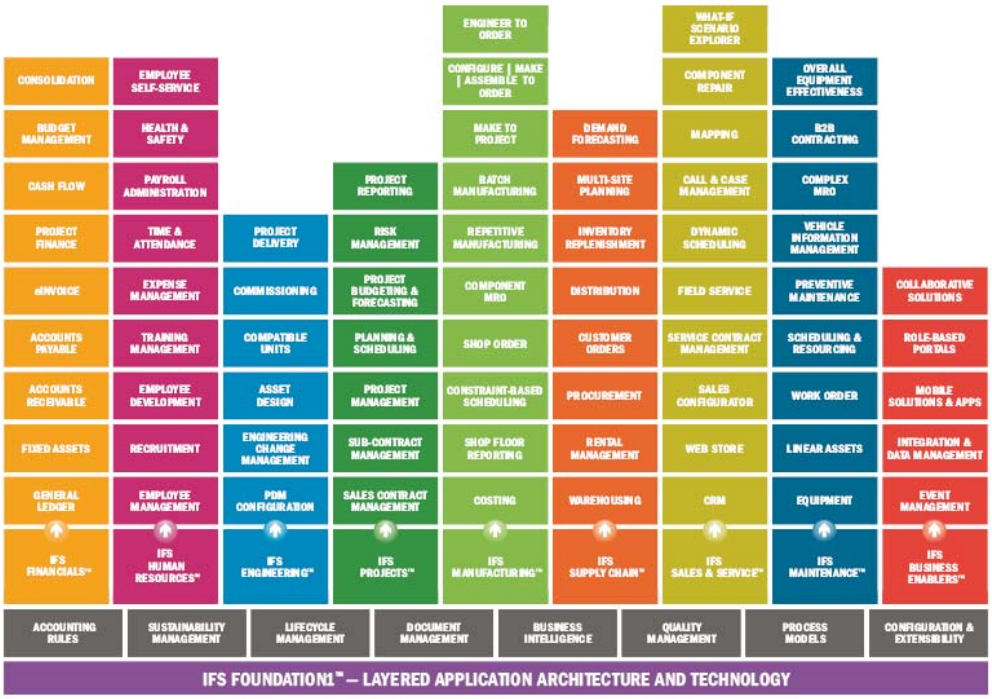
IFS incluye funcionalidades para la gestión financiera, recursos humanos, gestión de calidad, gestión documental, CRM, business intelligence, sostenibilidad y otras importantes funcionalidades para la gestión de todo el ciclo de vida de productos, activos, clientes y proyectos.

La Figura 3.16 muestra la arquitectura y las funcionalidades del IFS. Cabe recalcar que el sistema posee infinidad de servicios en diferentes campos, en el caso de La Corporación los módulos que se encuentran implementados y funcionando desde el año 2012 son los siguientes:

- Gestión Financiera
- Gestión Documental
- Gestión de Activos

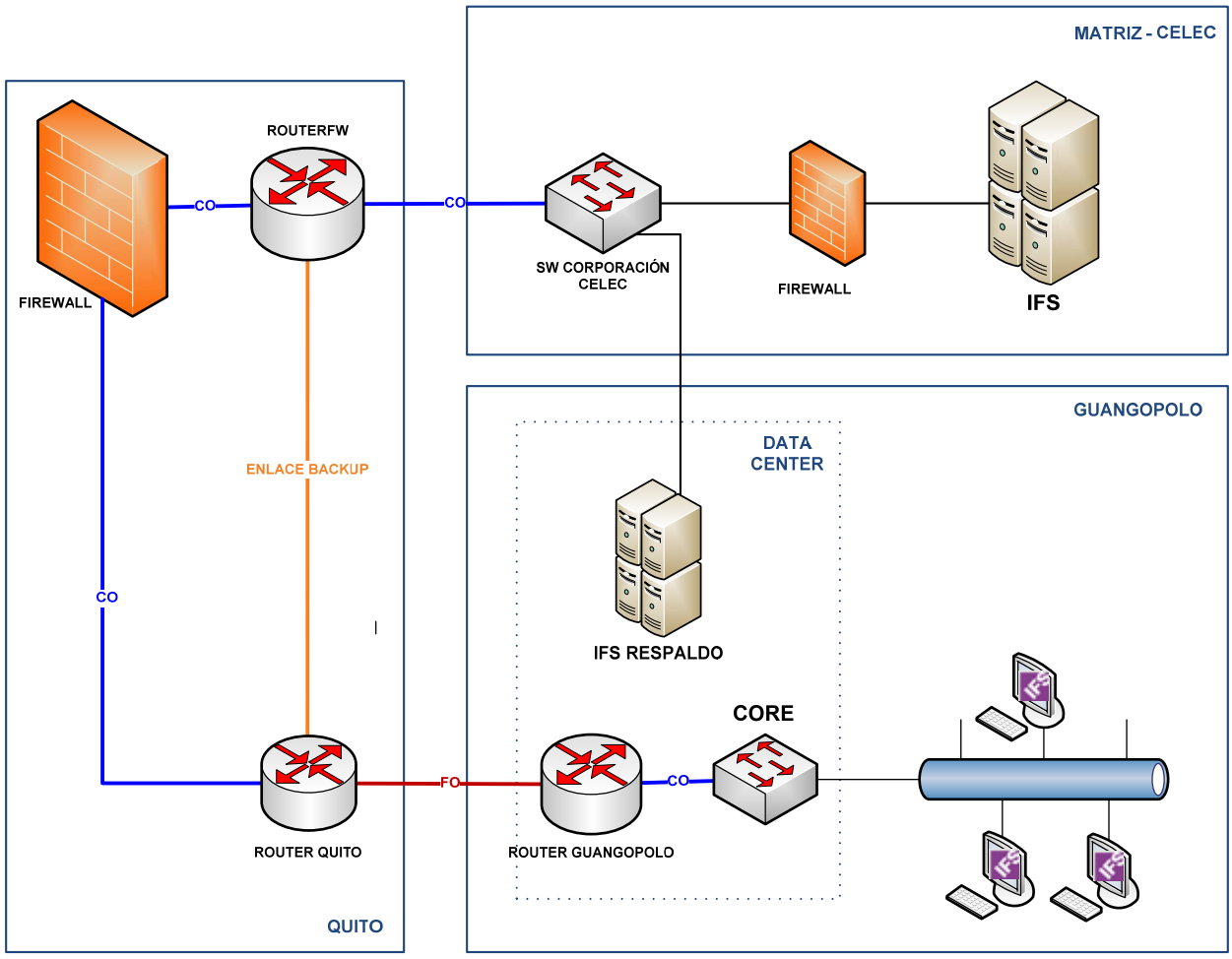
- Gestión de Bienes e Inventarios
- Gestión de Proyectos.

Figura 3. 16 Arquitectura y Aplicaciones del IFS



El IFS fue implementado a nivel de Corporación con el objetivo de mantener un solo sistema ERP para todas las Unidades de Negocio que la conforman, como también para incrementar la productividad, reducción de costos, mayor claridad en los procesos del negocio e información centralizada.

Figura 3. 17 Infraestructura de red IFS



En la Figura 3.17 se muestra la infraestructura de red de Termopichincha hacia el IFS ubicado en la Unidad Matriz de la Corporación, en la cual, los servidores principales se encuentran atrás del switch Corporativo, seguido de un firewall y adicionalmente se tienen servidores de respaldos ubicados en el Data Center de Termopichincha. Nuestra infraestructura WAN permite la conexión hacia este servicio por medio de los Routers de Guangopolo, Quito y Routerfw. Dentro de nuestra LAN los usuarios se conectan al servicio mediante HTTP hacia la dirección IP de los servidores y se comunican por la WAN. Es importante aclarar que a pesar de

ser un servicio Corporativo, todo el tráfico está pasando por el Firewall en Quito, en el caso que el enlace de Backup entre a funcionar, el tráfico ya no pasa por el Firewall.

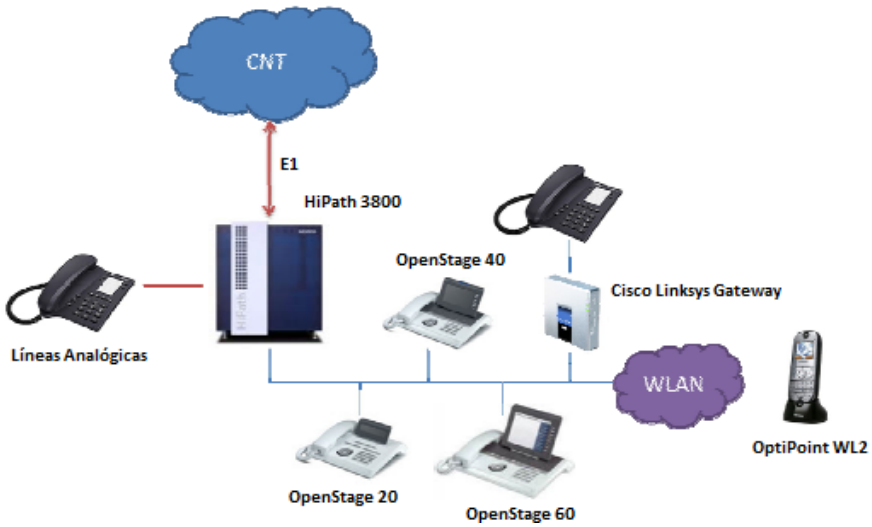
3.4.2 Telefonía IP

La arquitectura actual de telefonía se encuentra implementada bajo la marca Siemens con un equipo HiPath 3800 con una versión del sistema V8.0 que soporte 220 extensiones repartidas entre IP, SIP y analógicas.

Las líneas troncales principales están conformadas por una E1 la cual es contratada por CNT mediante un canal de fibra óptica. Y una troncal de 8 líneas telefónicas en el caso de caídas del servicio.

Existen actualmente 157 clientes IP configurados, 9 clientes SIP y 170 buzones de voz asignados tanto para los clientes IP, SIP como para la PBX.

Figura 3. 18 Distribución de red de la telefonía IP (Diagrama Proveedor HithTelecom, 2010)



En la Figura 3.18 se presenta la arquitectura defina por el proveedor durante la implementación de la solución con los modelos de los equipos que forman parte de la solución.

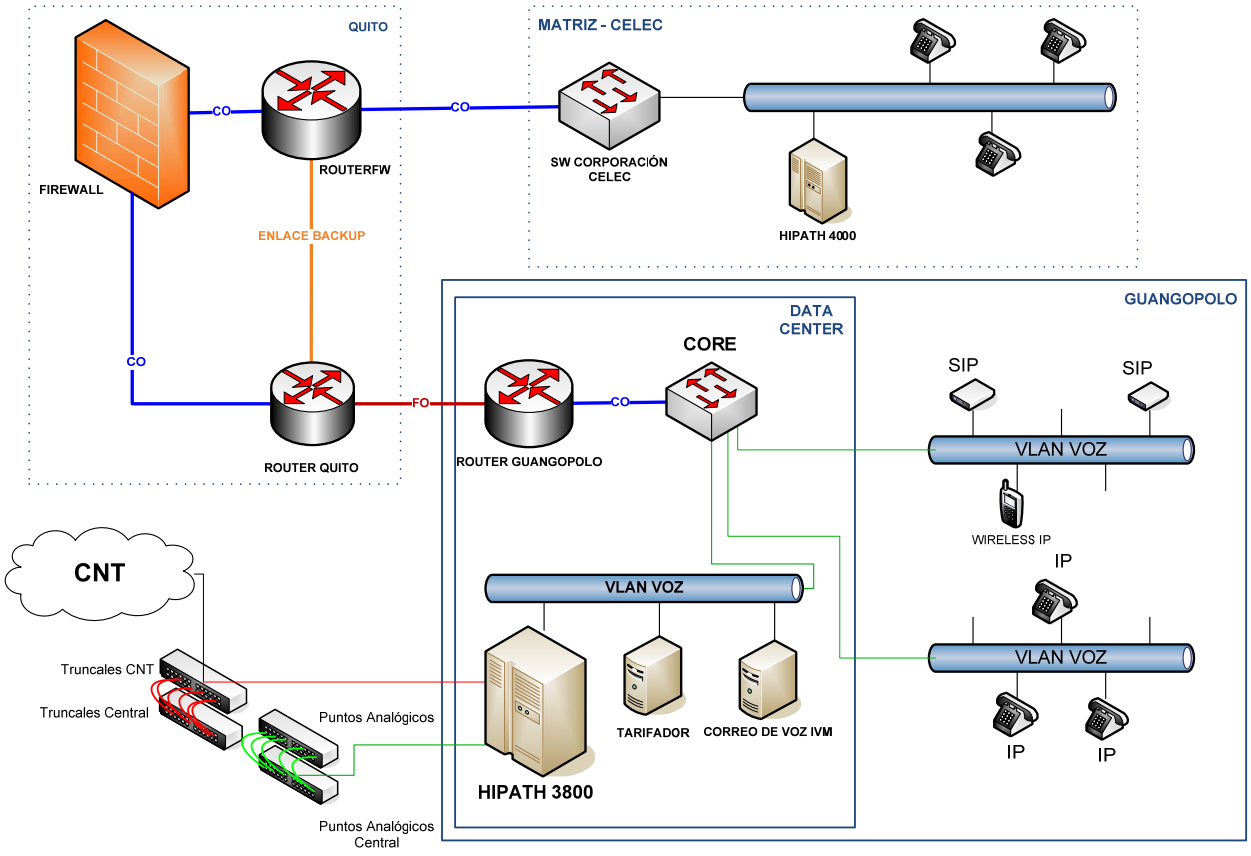
Debido a la necesidad de la comunicación directa con la Unidades de Negocios Transelectric, la central telefónica mantiene una conexión directa con la central telefónica de dicha unidad. Mediante la marcación de un código la central telefónica establece la conexión directa permitiendo que se realice las llamadas a las extensiones de la otra central. Esta conexión la realiza utilizando el enlace WAN mantenido hacia la corporación.

Como parte de la solución de telefonía se mantiene dos servidores los cuales prestan los servicios de buzón de voz y tarifador. Toda la infraestructura red de telefonía maneja una VLAN dedicada únicamente para voz.

Las estaciones de trabajo de los usuarios en algunos caso se encuentran conectadas directamente en los terminales IP ya que estos poseen una interfaces de red adicional a su conexión. Esta interface de red realiza la función de switch dentro del terminal.

Los modelos OpenStage 20, 40 y 60 utilizados en los clientes brindan funcionalidades de QoS que pueden ser configuradas dentro del software. Tecnologías de QoS a nivel de capa 2 y tecnologías de QoS a nivel de capa 3 como Diffserv y TOS/IP Precedence permitiendo a la VoIP mejorar en capacidad de ancho de banda, latencia y nivel de servicio.

Figura 3. 19 Infraestructura de red de la telefonía IP



En la Figura 3.19 se muestra la infraestructura de telefonía que se maneja y la conexión hacia la central telefónica de la Corporación. Desde el switch de CORE se genera una VLAN dedicada para el servicio, en donde la central telefónica HIPATH 3800 se conecta con los servidor de Correo de Voz, el Tarifador y todos los dispositivos de telefonía IP. Mediante un canal dedicado de CNT (E1) se realiza la conexión de las troncales hacia la central telefónica. Adicionalmente se manejan puertos analógicos conectadas a la central. Para establecer la comunicación hacia la Corporación, todo el tráfico viaja a través de la WAN por medio de los Routers de Guangopolo, Quito y Routerfw. Igualmente todo el tráfico pasa por el Firewall en Quito, en el caso que el enlace de Backup entre a funcionar, el tráfico ya no pasa por el Firewall.

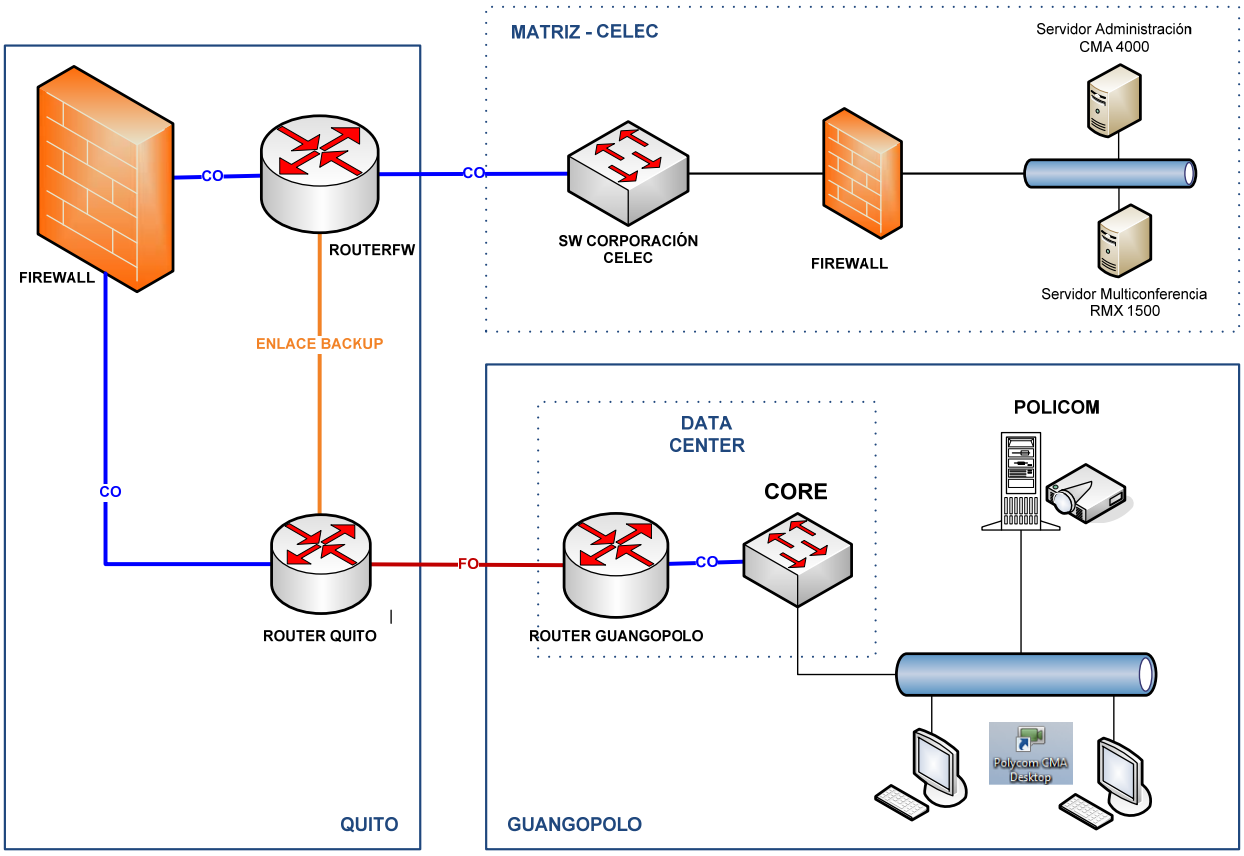
3.4.3 Videoconferencia

El sistema de videoconferencia se encuentra implementado a nivel de la Corporación, en donde cada Unidad de Negocios mantiene un o dos equipos de videoconferencia Polycom que se conectan mediante los diferentes enlaces WAN hacia los servidores de videoconferencia.

En el caso de la Unidad de Negocios Termopichincha se tiene un solo equipo de videoconferencia Polycom HDX 7000 HD ubicado dentro de la red LAN en la sala de reuniones de la Gerencia de la Unidad. Para el manejo de la videoconferencia en los diferentes usuarios se tiene como parte de la solución clientes licenciados del software Polycom CMA Desktop. Este cliente permite realizar videoconferencias directamente con el equipo Polycom o entre clientes. Entre las características más importante de los clientes CMA tenemos:

- Mostrar la pantalla del ordenador durante la videoconferencia.
- Mantener una lista de contactos.
- Formar parte de una videoconferencia con varios integrantes.
- Fácil de usar.

Figura 3. 20 Infraestructura de red de la videoconferencia



En la Figura 3.20 se muestra la infraestructura de videoconferencia que se maneja y la conexión hacia la Corporación. El equipo Polycom se encuentra conectado a la red dentro de la VLAN dedicada para servidores, los usuarios mediante sus clientes de videoconferencia se conectan en la LAN y pueden establecer comunicación con el equipo Polycom. Para establecer la comunicación hacia la Corporación, el equipo Polycom se registra en los servidores CMA y RMX utilizando el canal de comunicación WAN por medio de los Routers de Guangopolo, Quito y Routerfw. Igualmente todo el tráfico pasa por el Firewall en Quito, en el caso que el enlace de Backup entre a funcionar, el tráfico ya no pasa por el Firewall.

3.4.4 Scada

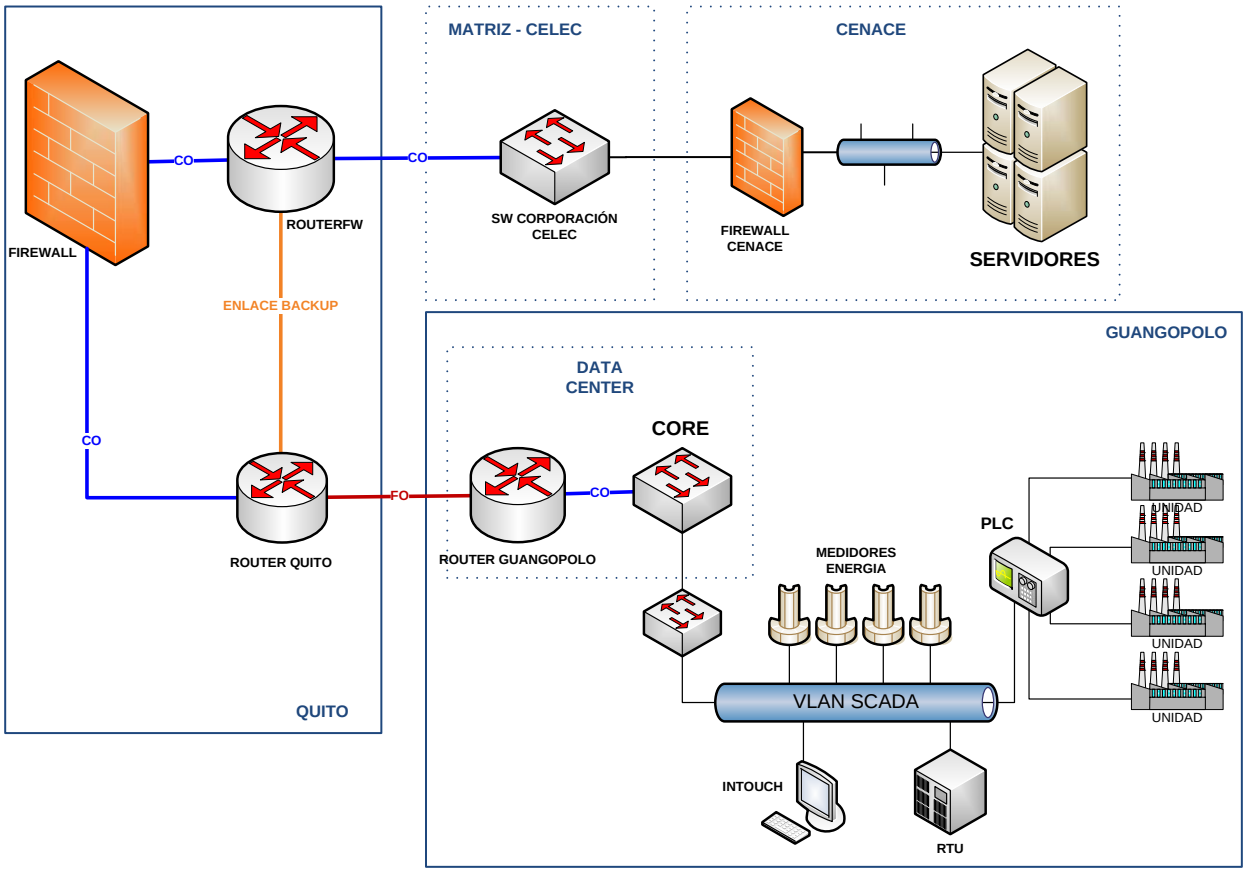
El sistema scada se encuentra implementado en cada una de las unidades de generación térmica que conforma la Unidad de Negocios Termopichincha. Se manejan alrededor de 10 centrales termicas ubicadas en diferentes partes del país.

El sistema scada permite realizar un control y supervisión automática de todos los procesos industriales mediante dispositivos como sensores, medidores, rtu y obtener datos en tiempo real. La información puede ser manejada en bases de datos o distribuida por la red para la manipulación y estructuración de informes, reportes y bitácoras.

Toda la información generada por los sistemas industriales se la categoriza como crítica dentro de la Unidad de Negocios Termopichincha ya que es controlada, monitoreada y evaluada por la entidad privada CENACE (Centro Nacional de Control de Energía), que es la principal organización de control en el tema de generación, distribución y comercialización de la energía.

En nuestro caso CENACE realiza el monitoreo en línea de la información industrial generada los 12 meses del año, las 24 horas al día hacia todas las unidades de generación (motores).

Figura 3. 21 Infraestructura de red de scada



En la Figura 3.21 se muestra la infraestructura del sistema scada. La red industrial es manejada con una VLAN Scada dedicada generada por el switch de CORE, en la cual están conectados todos los dispositivos industriales como: RTU (Unidad Terminal Remota), medidores de energía, PLC (Controladores Lógicos Programables) y el sistema INTOUCH. Para establecer la comunicación hacia las entidades públicas reguladoras se utiliza el canal de comunicación WAN por medio de los Routers de Guangopolo, Quito y Routerfw. Igualmente todo el tráfico pasa por el Firewall en Quito, en el caso que el enlace de Backup entre a funcionar, el tráfico ya no pasa por el Firewall. En el caso de CENACE, los servidores recolectan la información de generación desde su infraestructura hacia la infraestructura de Termopichincha por el canal WAN.

3.4.5 Aplicaciones Lotus

Los diferentes servicios que brindan los aplicativos Lotus son basados en un desarrollo Lotus Designer y una infraestructura Lotus Domino.

Lotus Domino/Lotus Notes es una plataforma de comunicación, colaboración, mensajería, software de aplicaciones web que proveen una infraestructura escalable, segura y flexible, y permite compartir bases de datos con información, como bases documentales, de procedimientos, manuales o foros de discusión.

Lotus Domino permite manejar un ambiente integrado de Cliente/Servidor. La integración la puede realizar entre clientes Lotus Notes y las No-Notes. El ambiente de Lotus Notes y del Domino proporciona servicios para permitir a la Unidad de Negocios Termopichincha realizar tareas de almacenamiento, de comunicación y de intercambio de la información.

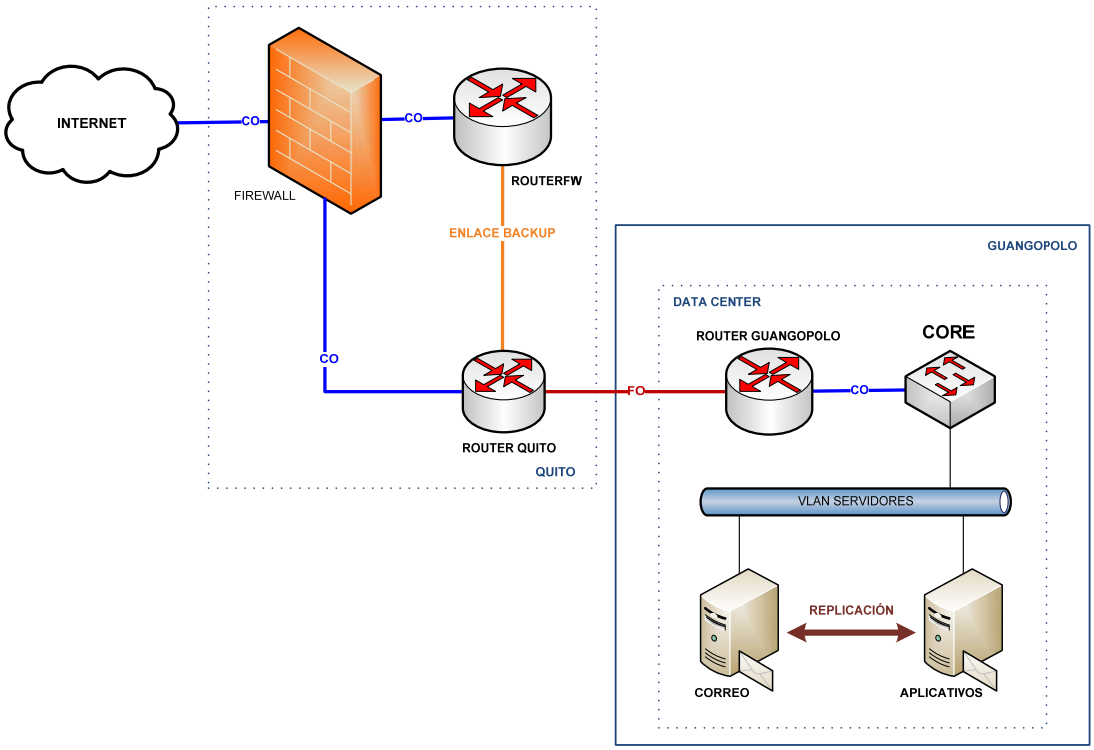
Las aplicaciones de Lotus Domino permiten compartir, recopilar, controlar y organizar la información utilizando Lotus Notes y otros clientes de uso universal. La información puede estar incluida en bases de Notes o en aplicaciones heredadas.

Dentro de la Unidad de Negocios Termopichincha se manejan alrededor de 20 aplicativos que prestan servicios de Memos y Oficios, Memos y Oficios, Gestión Organizacional, Facturas y contratos, RBS, Portal del Conocimiento, Proceso de Compras Públicas, RRHH, Permisos de Trabajo, Generación en Tiempo Real, Mesa de Servicios, Laboratorio, Valija, Proveedores, Seguros y Gestión social y Ambiental.

Figura 3. 22 Aplicativos Internos Lotus

En la Figura 3.23 se muestra la infraestructura Domino con respecto a los Aplicativos internos. Los servidores de Domino Aplicativos y Correo se encuentran dentro de la misma VLAN de Servidores lo cual permite la sincronización de información entre ambos. Los usuarios mediante clientes Lotus Notes establecen la comunicación dentro de la misma LAN interna y pueden consumir los servicios. Para establecer la comunicación hacia los servidores desde sitios remotos se utiliza el canal de comunicación WAN por medio de los Routers de Guangopolo, Quito y Routerfw. Igualmente todo el tráfico pasa por el Firewall en Quito, en el caso que el enlace de Backup entre a funcionar, el tráfico ya no pasa por el Firewall.

Figura 3. 23 Infraestructura de red de los aplicativos Lotus



3.4.6 Correo Electrónico

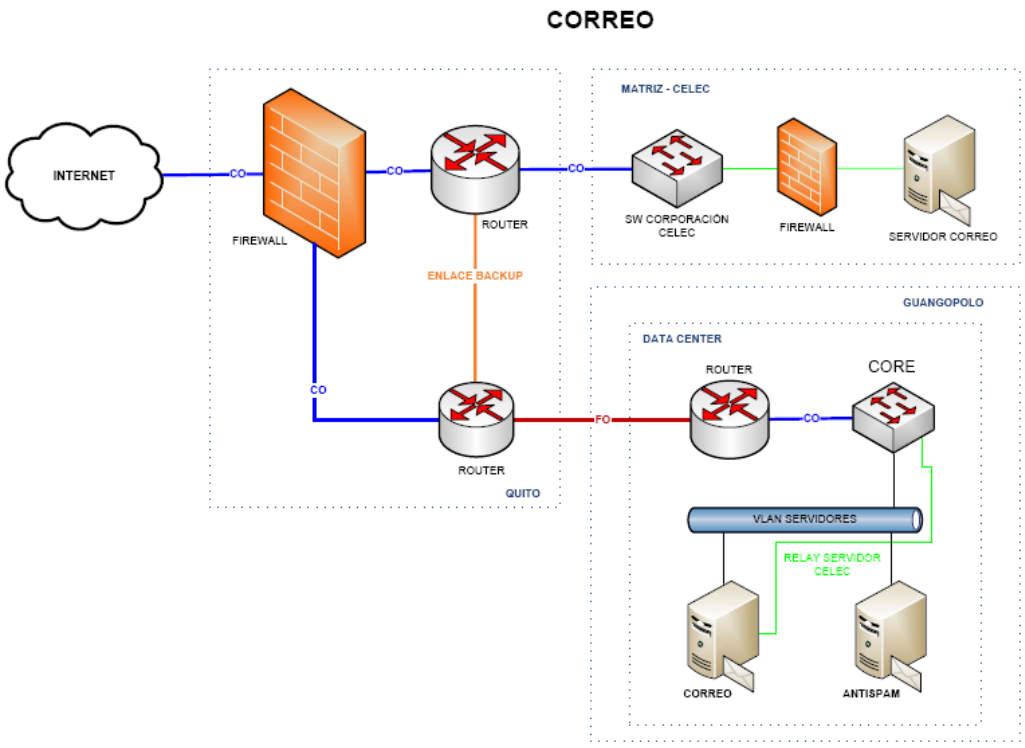
El servicio de correo electrónico se encuentra implementado bajo un servidor Lotus Domino dentro de la misma infraestructura Domino. En este caso el servidor Domino se encuentra cumpliendo funciones de envío y recepción de correo electrónico.

Mediante el uso de los clientes Lotus Notes los usuarios puedes acceder a las bases de correo electrónico, permitiendo que cada usuario pueda realizar la recepción y envío de correos mediante la sincronización de información con el servidor. Todos los correos generados internamente dentro de la infraestructura LAN son gestionados por el servidor de Correo.

La infraestructura actual permite que los correos generados hacia destinos externos no salgan directamente al internet sino que sean replicados (Relay) directamente hacia el servidor de correo

de la Corporación utilizando los enlaces WAN, esto debido a políticas internas establecidas dentro de la Corporación.

Figura 3. 24 Infraestructura de red del correo electrónico



En la Figura 3.24 se muestra la infraestructura Domino con respecto al correo electrónico. Los servidores de Domino Correo y Antispam se encuentran dentro de la misma VLAN de Servidores lo cual permite la sincronización de información entre ambos. Los usuarios mediante clientes Lotus Notes establecen la comunicación dentro de la misma LAN interna y pueden consumir los servicios de correo. En el caso del correo externo, se puede observar que el servidor de correo realiza el relay hacia el servidor de correo Corporativo utilizando el canal de comunicación WAN por medio de los Routers de Guangopolo, Quito y Routerfw. Igualmente todo el tráfico pasa por el Firewall en Quito, en el caso que el enlace de Backup entre a funcionar, el tráfico ya no pasa por el Firewall.

3.5 Análisis y Clasificación del Tráfico

Dentro de la infraestructura de red de la Unidad de Negocios Termopichincha se ha realizado un análisis de la red para identificar los tipos de tráfico, protocolos, puertos y ancho de banda que se presentan dentro de los diferentes enlaces y estaciones de trabajo, dentro y fuera de horarios de trabajo. Es importante aclarar que el análisis de tráfico se lo realiza durante los meses de Mayo y Junio del 2015, los cuales presentan mayor movimiento en los servicios de red debido a los siguientes puntos:

- **Subgerencia Financiera:** Dentro de la Unidad de Negocios se genera un cronograma de cumplimiento de procesos financieros, los cuales son realizados en los últimos días del mes y comienzos del siguiente:

Tabla 3. 5 Cronograma Financiero de Cierre de mes - MAYO

CRONOGRAMA DE CIERRE MAYO DEL 2015

RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD	FECHA MAXIMA
INVENTARIOS Y BODEGAS	REVISIÓN Y DEPURARION DE RBS	22/05/2015
ADQUISICIONES	ENTREGA DE DOCUMENTACION DE IMPORTACIONES.	22/05/2015
RESPONSABLES DE FONDOS Y CAJA CHICAS	LIQUIDACIÓN DE FONDOS / CAJAS CHICAS	23/05/2015
LOGISTICA	CIERRE DE ELABORACION DE ORDENES DE COMPRA	20/05/2015
PRESUPUESTO	CIERRE DE CERTIFICACION PRESUPUESTARIA DE ORDENES DE	23/05/2015

	COMPRA Y NOTIFICACION	
RRHH	ENTREGA DE ROL DE PAGOS, ANEXOS DE PROVISIONES, ARCHIVOS PARA PAGO.	23/05/2015
ARCHIVO	CIERRE DE ARCHIVO FACTURACION (recepción de facturas originales excepto combustible de generación)	22/05/2015
RRHH	CIERRE DE EMISIÓN DE FACTURAS DE VIATICOS	22/05/2015
TODOS LOS RESPONSABLES	**RECEPCION DE FACTURAS DE PROVEEDORES,**	22/05/2015
ADQUISICIONES	INFORME CIERRE ORDENES DE COMPRA EN EL IFS BIENES	25/05/2015
TODOS LOS RESPONSABLES	CIERRE DE RECEPCION DE ORDENES DE COMPRA DE SERVICIOS	24/05/2015
PRESUPUESTO	REPORTE DE ESTADO DE ORDENES DE COMPRA A CONTABILIDAD	26/05/2015
CONTABILIDAD	CIERRE DE REGISTRO CONTABLE DE FACTURAS	28/05/2015
CONTABILIDAD	BASE DE DATOS ROL DE PAGOS	24/05/2015
CONTABILIDAD	CIERRE DE COMPROBANTES DE RETENCION	02/06/2015
CONTABILIDAD	CONCILIACION ANTICIPOS REMUNERACIONES	02/06/2015

TESORERIA	CERTIFICACIÓN Y OBLIGACIONES PENDIENTES DE PAGO AL 28/05/2015	09/06/2015
TESORERIA	CONCILIACION DE BANCOS	04/06/2015
INVENTARIOS Y BODEGAS	CIERRE DE MODULO DE ACTIVOS FIJOS	28/06/2015
INVENTARIOS Y BODEGAS	CONCILIACION BODEGAS Y CIERRE DE MODULO DE INVENTARIOS	02/06/2015
CONTABILIDAD	CONCILIACION DE ACTIVOS FIJOS Y DEPRECIACIÓN.	03/06/2015
TESORERÍA	REPORTE DE BENEFICIARIOS	04/06/2015
TESORERÍA	EJECUCION FLUJO DE CAJA	06/06/2015
CONTABILIDAD	REGISTRO Y AMORTIZACION DE SEGUROS	06/06/2015
CONTABILIDAD	CONCILIACION FACTURAS MODULO DOCUMENTAL FACTURAS IFS	06/06/2015
TESORERIA	CIERRE DE PAGOS CON PETROECUADOR	06/06/2015
TESORERIA	CONCILIACION CUENTAS POR PAGAR CON PETROECUADOR	09/06/2015
TESORERÍA	CONCILIACION GARANTIAS ANTICIPO DE REMUNERACIONES	10/06/2015
CONTABILIDAD	CONCILIACION Y CIERRE DE MODULO DE CUENTAS POR PAGAR	10/06/2015

CONTABILIDAD	CONCILIACION DE TRANSFERENCIAS INTERNAS CON CELEC EP MATRIZ	10/06/2015
CONTABILIDAD	REPORTE DE IMPUESTOS A CELEC EP	10/06/2015
CONTABILIDAD	REVISION DE SALDOS Y DEPURACIÓN DE CUENTAS	10/06/2015
CONTABILIDAD	REVISIÓN DE BALANCES PROVISIONALES MENSUAL	10/06/2015
CONTABILIDAD	EMISION DE BALANCES DEFINITIVOS	11/06/2015
CONTABILIDAD	LIQUIDACION DE EJECUCION CONTRATO GALAPAGOS	10/06/2015
CONTABILIDAD	LIQUIDACIÓN INVERSIÓN GUANGOPOLO II	10/06/2015
SUBG PRODUCCION	REPORTE DE INGRESOS DE GENERACION DE MAYO 2015	13/06/2015
CONTABILIDAD	INFORME DE COSTOS MENSUAL	13/06/2015
PRESUPUESTO	INFORME DE EJECUCIÓN PRESUPUESTARIA	11/06/2015
CONTABILIDAD	ENTREGA TRAMITE DE FACTURAS.	PERMANENTE

- Los procesos de cierre de facturas son realizados a partir del 22 de cada mes, según disposición realizada por la Subgerencia Financiera, mediante memorando interno TPI-SF-0746-15. Esto provoca que a partir de dicha fecha se tenga mayor carga de trabajo en el área financiera, con la participación de distintas áreas de la Unidad.

- Dentro de la validación de las bases de facturación manual de proveedores realizada el mes de Junio 2015, se identifica que el valor más alto se presenta en el mes de Mayo, causando un alto porcentaje de procesos transaccionales realizados durante este tiempo.

Figura 3. 25 Validación de las bases de facturación de proveedores

Suma de Imp Brut		Fecha Asie						
Validación	Serie	ene	feb	mar	abr	may	jun	Total general
DECLARADO	1	4.274.116,24	6.087.976,87	6.974.054,08	8.045.297,12	4.662.674,68	6.572.517,44	36.616.636,43
	2	2.630,00	2.630,00	2.327,50	1.225,00		78,00	8.890,50
	3	1.335,39		3.876,92	5.491,79	3.838,75	73.148,65	87.691,50
	41		5.270,44	36.557,15	155.123,20	1.825,90	10.081,87	208.858,56
	04_PRE		-868,00	-57,34	-880,49	-789,57	-3.651,28	-6.246,68
	5					21,50		21,50
	01_PRE						46.402,66	46.402,66
Total DECLARADO		4.278.081,63	6.095.009,31	7.016.758,31	8.206.256,62	4.667.571,26	6.698.577,34	36.962.254,47
NO DECLARADA	1						18.060,82	18.060,82
	OTROS	575,85	227.145,54	4.338.504,25	1.277.036,54	6.874.600,74	1.065.140,17	13.783.003,09
	OTROS_1	25.327,21	37.289,10	60.180,49	20.781,49	430.580,92	301.359,97	875.519,18
	RRHH	486.274,57	133.700,49	135.682,08	145.708,36	138.278,00	132.375,69	1.172.019,19
	RRHH_A	1.206.156,60	1.279.704,48	1.391.464,30	1.380.904,80	1.628.342,92	1.402.442,02	8.289.015,12
	RRHH_B	821.113,74	1.165.629,35	1.216.987,86	1.231.578,37	1.444.576,43	1.320.966,72	7.200.852,47
Total NO DECLARADAS		2.539.447,97	2.843.468,96	7.142.818,98	4.056.009,56	10.516.379,01	4.240.345,39	31.338.469,87
IMPORTACION	OTROS	83.006,85	1.716.553,11	420.576,95	1.746.077,26		44.018,56	4.010.232,73
	OTROS_1				835.722,44			835.722,44
Total IMPORTACION		83.006,85	1.716.553,11	420.576,95	2.581.799,70		44.018,56	4.845.955,17
Total general		**6.900.536,45**	**10.655.031,38**	**14.580.154,24**	**14.844.065,88**	**15.183.950,27**	**10.982.941,29**	**73.146.679,51**

- **Subgerencia de Gestión Organizacional:** Durante el mes de mayo se solicita dar cumplimiento a la disposición por parte de la Dirección de Gestión Estratégica a todas las área de la Unidad, el cual, tiene como objetivo la preparación de las fichas técnicas de cada una de las Inversiones de Gestión Operativa para el año 2016, con un plazo de entrega muy corto, provocando un alto consumo de los recursos de red y comunicación entre las distintas áreas.

  Adicionalmente la Unidad maneja un Sistema de Gestión de Calidad, en donde el registro de la información de las metas, indicadores y demás es realizada mensualmente, trimestralmente y semestralmente, provocan mayor carga de registro

de información en los sistemas internos y externos, en especial el registro del GPR (Gobierno por Resultados).

- **Jefatura de Adquisiciones:** Durante el mes de mayo se entrega el Informe de Ejecución del PAC (Plan Anual de Contratación) del primer cuatrimestre del año 2015, con el objetivo de que las áreas que no hayan cumplido con la ejecución de sus proyectos, lo realizen de manera inmediata o se presente un justificativo del no cumplimiento.
- **Subgerencia de Producción:** Durante el mes de mayo y junio se presentan dos eventos considerados de mayor importancia dentro de la Central Guangopolo que constan dentro de la Declaración de Mantenimiento del Plan de Operación. En el mes de mayo se programa la PARADA DE PLANTA anual de la Central Guangopolo y en el mes de junio la PARADA DE PLANTA anual de la Central Guangopolo II. Estos eventos provocan mayor flujo de comunicación y utilización de los servicios de red.

Figura 3. 26 Cronogramas de Paradas de Central Guangopolo y Guangopolo II

NOMBRE DE LA CENTRAL: Central Térmica GUANGOPOLO I

CENTRAL Y/O UNIDAD	MES	FECHA DE INICIO	FECHA DE TERMINACIÓN	DÍAS DE DURACIÓN	POTENCIA RESTRINGIDA (MW)	BREVE DESCRIPCIÓN DEL TRABAJO
PARADA PLANTA 2015	MAYO	11-may-15	31-may-15	21	21,80	PARA DE PLANTA ANUAL 2015
PARADA PLANTA 2016	MAYO	09-may-16	29-may-16	21	21,80	PARA DE PLANTA ANUAL 2016

NOMBRE DE LA CENTRAL: Central Térmica GUANGOPOLO II

CENTRAL Y/O UNIDAD	MES	FECHA DE INICIO	FECHA DE TERMINACIÓN	DÍAS DE DURACIÓN	POTENCIA RESTRINGIDA (MW)	BREVE DESCRIPCIÓN DEL TRABAJO
PARADA PLANTA 2015	JUNIO	01-jun-15	21-jun-15	21	21,80	PARA DE PLANTA ANUAL 2015
PARADA PLANTA 2016	MAYO	30-may-16	19-jun-16	21	21,80	PARA DE PLANTA ANUAL 2016

- **Jefatura de TIC:** Durante el mes de mayo y junio se da cumplimiento al Plan de Mantenimiento Preventivo del primer semestre dentro de la Central Guangopolo. El Plan también cubre actividades de mantenimiento en los destinos sitios remotos.

Figura 3. 27 Plan de Mantenimiento anual TIC

PLAN DE MANTENIMIENTO (1er SEMESTRE 2015)

Lugar (Oficinas / Centrales)	Mantenimiento Preventivo Primer Semestre 2015										
	ABRIL		MAYO				JUNIO				
	III	IV	I	II	III	IV	I	II	III	IV	Responsable
Quito	21										2 técnicos
GPO						25 al 29		8 al 12	15 al 19	22 al 26	todos
Santa Rosa		28									2 técnicos
Celso, Lumbaqui, Secoya			6,7,8								2 técnicos
Loreto, Dayuma, Payamino, Sacha, Jivino I,II y III					18 al 22						2 técnicos
Galápagos							2 al 5				2 técnicos
Quevedo II y Puna (respectivamente)		25,26				27,28					1 técnico

Fecha Planificada

Fecha tope de mantenimiento en caso de no cumplir en la planificada

- Mediante un reporte de la central telefónica, se puede apreciar el resumen de llamadas realizadas durante los meses de mayo y junio, teniendo un promedio total de 16000 llamadas aproximadamente.

Figura 3. 28 Reportes Central Telefónica Mayo y Junio

Report Type: Overall Summary			
Extension: All			
Filters: Mon-Fri, Outgoing Calls, Sat-Sun			
Reporting Period: 1/5/2015 00:01:00 - 31/5/2015 23:59:00			
	Number	Duration	Cost
		hh:mm:ss	€
Call Totals			
Total Calls	17876	403:29:34	2707,33
Total Answered	17841	403:29:34	2707,33
Total Unanswerec	35	0:00:00	0,00
Call Type			
Outgoing (Answe	7205	280:16:09	2707,33
Incoming (Answe	10636	123:13:25	0,00
Incoming (Unans	35	0:00:00	0,00
Destination of Answered Outgoing Calls			
Local	4120	170:24:22	370,58
Nacional	418	18:17:04	161,25
Internacional	7	0:29:35	14,26
Regional	287	13:09:55	52,87
Celular	2373	77:55:13	2108,37
Carrier Totals for Answered Outgoing Calls			
Andinatel	7205	280:16:09	2707,33
Rate for Answered Outgoing Calls			
Estándar	7205	280:16:09	2707,33

Report Type: Overall Summary			
Extension: All			
Filters: Mon-Fri, Outgoing Calls, Sat-Sun			
Reporting Period: 1/6/2015 00:01:00 - 30/6/2015 23:59:00			
	Number	Duration	Cost
		hh:mm:ss	€
Call Totals			
Total Calls	14585	327:09:42	2023,38
Total Answered	14556	327:09:42	2023,38
Total Unanswered	29	0:00:00	0,00
Call Type			
Outgoing (Answer	5418	218:17:10	2023,38
Incoming (Answer	9138	108:52:32	0,00
Incoming (Unansw	29	0:00:00	0,00
Destination of Answered Outgoing Calls			
Local	3104	135:41:29	290,73
Nacional	313	15:42:28	136,42
Internacional	6	0:29:48	14,48
Regional	192	11:05:21	43,08
Celular	1803	55:18:04	1538,67
Carrier Totals for Answered Outgoing Calls			
Andinatel	5418	218:17:10	2023,38
Rate for Answered Outgoing Calls			
Estándar	5418	218:17:10	2023,38

Las herramientas utilizadas para realizar el escaneo e identificación de la red son: WhatsUp, Monitoreo Checkpoint y NBAR propietario de Cisco.

WhatsUp es una herramienta robusta de gestión y monitoreo de redes, aplicada durante las 24 horas del día, los 7 días a la semana, permitiendo simplificar las tareas de un administrador de red.

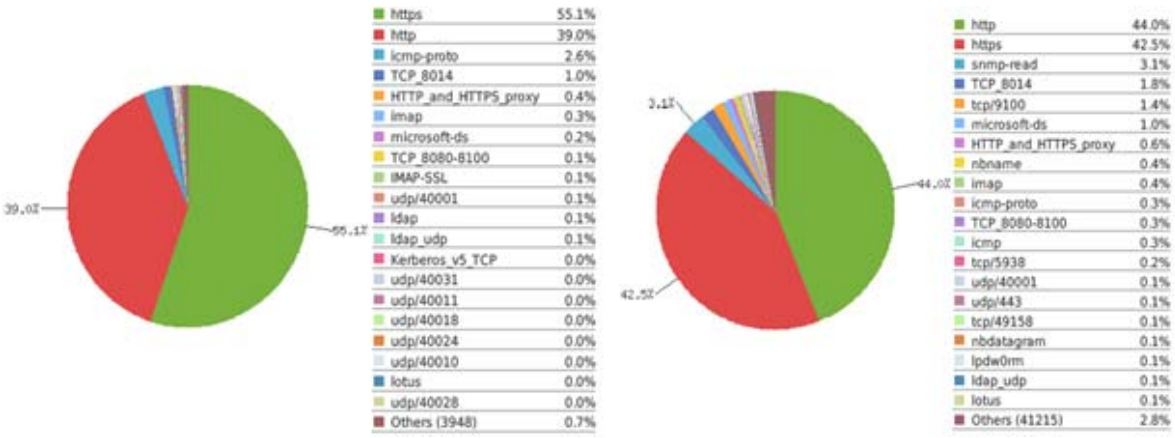
Monitoreo de Checkpoint es uno de los componentes que conforman toda una infraestructura de seguridad perimetral la cual permite realizar un escaneo profundo de todo el trafico de red que se presenta dentro de la infraestructura. Analiza todo el flujo de trabajo de la infraestructura de red identificando los diferentes puertos, protocolos y aplicaciones.

NBAR es un mecanismo introducido en los sistemas operativos de los equipos de comunicación (routers) que permite realizar una clasificación del tráfico y control de ancho de banda para las aplicaciones de red.

3.5.1 Tipos de Tráficos

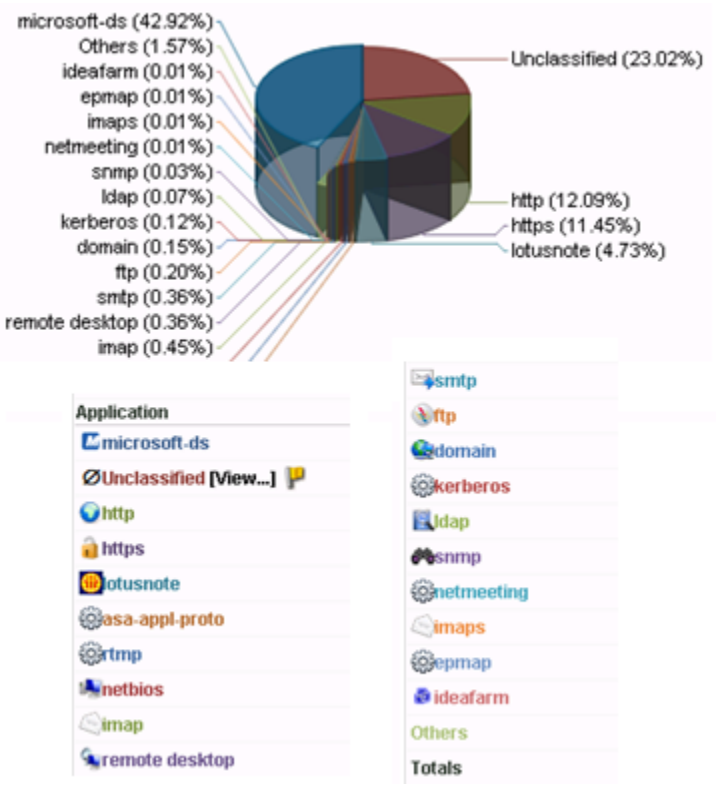
Mediante la utilización de la herramienta de Monitoreo de Checkpoint se pudo obtener el tipo de tráfico que circula dentro de la infraestructura de red de la Unidad de Negocios Termopichincha durante el mes de Mayo 2015. La figura 3.29 muestra los porcentajes y el tipo de tráfico.

Figura 3. 29 Tipos de tráfico (checkpoint)



Mediante la utilización de la herramienta WhatsUp se pudo obtener el tipo de tráfico que circula dentro de la infraestructura de red de la Unidad de Negocios Termopichincha durante una semana del mes de Junio 2015. La figura 3.30 muestra los porcentajes y el tipo de tráfico.

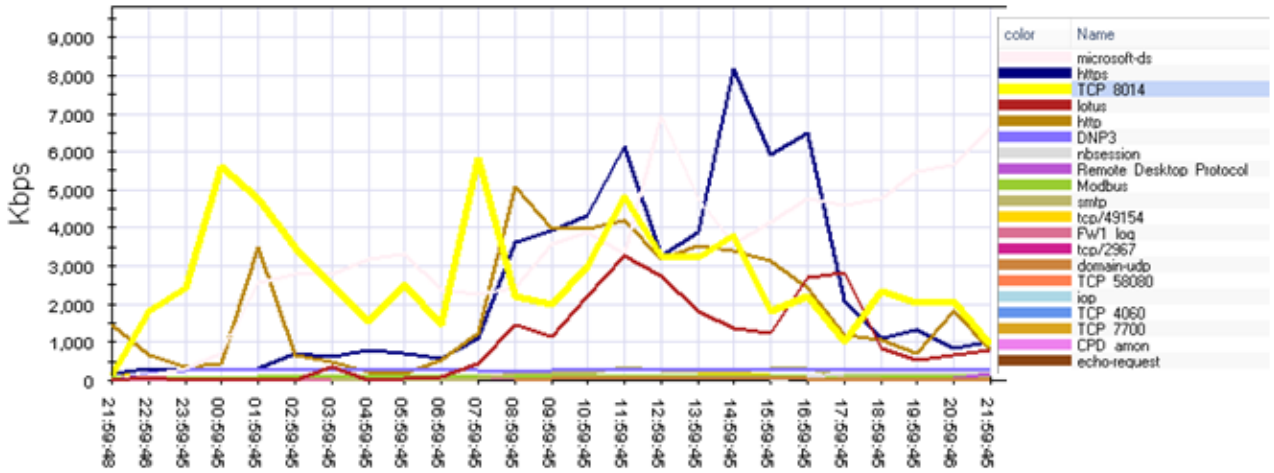
Figura 3. 30 Tipos de tráficos (whatsup)



Para tener una idea del tipo de tráfico que circula a diario durante los horarios dentro y fuera de oficina, se realizó un monitoreo durante los 7 días de la semana, las 24 horas del día, mediante la herramienta de monitoreo de checkpoint. Las siguientes figuras muestran el tipo de tráfico generado.

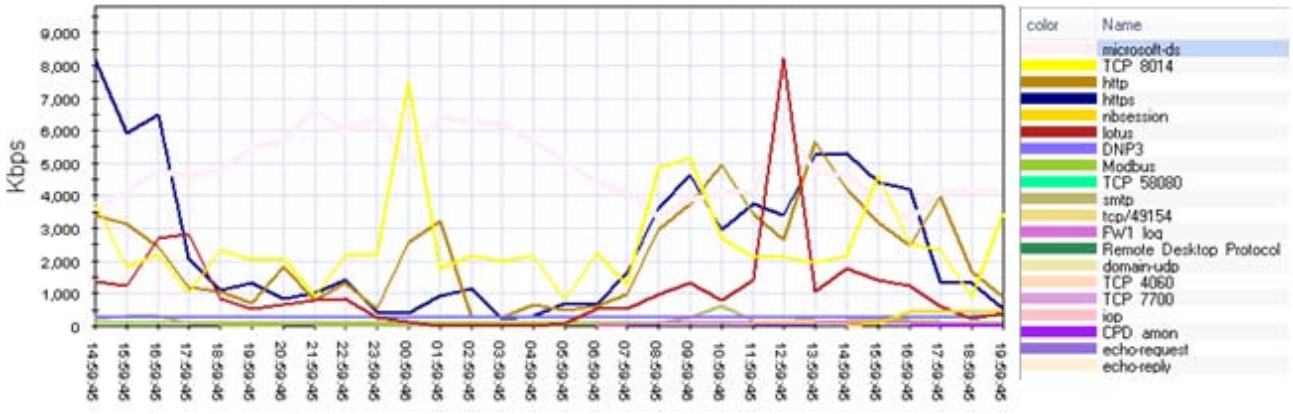
En el caso de la Figura 3.31, el tráfico que presenta mayor consumo es el protocolo HTTPS el cual se mantiene entre los 3 MB hasta superar los 8 MB provocando una saturación del canal ya que el ancho de banda en cuanto a internet es de 8 MB para toda la Unidad de Negocios Termopichincha. Debido a que es el primer día de la semana el tráfico aumenta considerablemente.

3. 31 Tipo de Tráfico - Del lunes 1 al martes 2 de Junio 2015



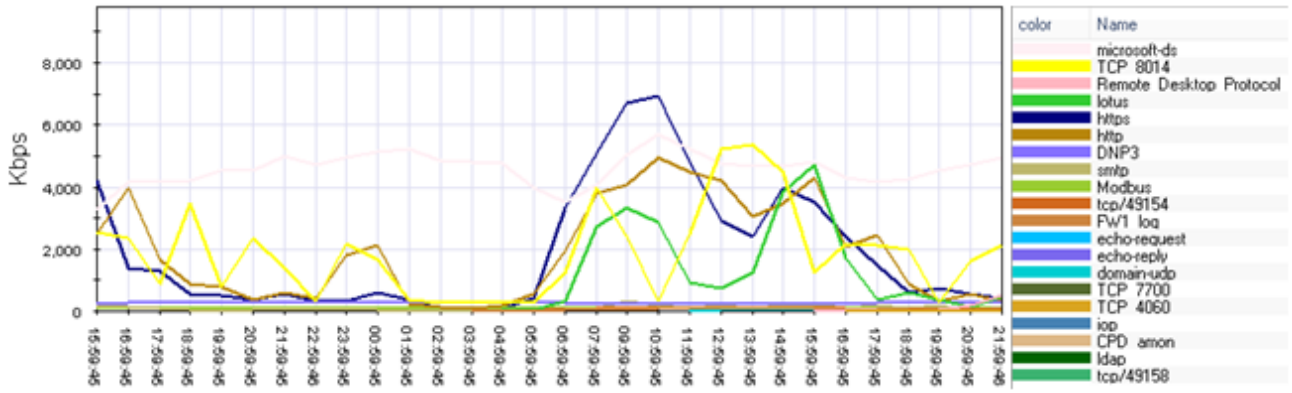
En el caso de la Figura 3.32, el tráfico que presenta mayor consumo es el protocolo LOTUS, el cual supera los 8 MB provocando que la disponibilidad del servicio se encuentre activo. Los protocolos HTTP y HTTPS presentan un consumo moderado

Figura 3. 32 Tipo de Tráfico - Del martes 2 al miércoles 3 de Junio 2015



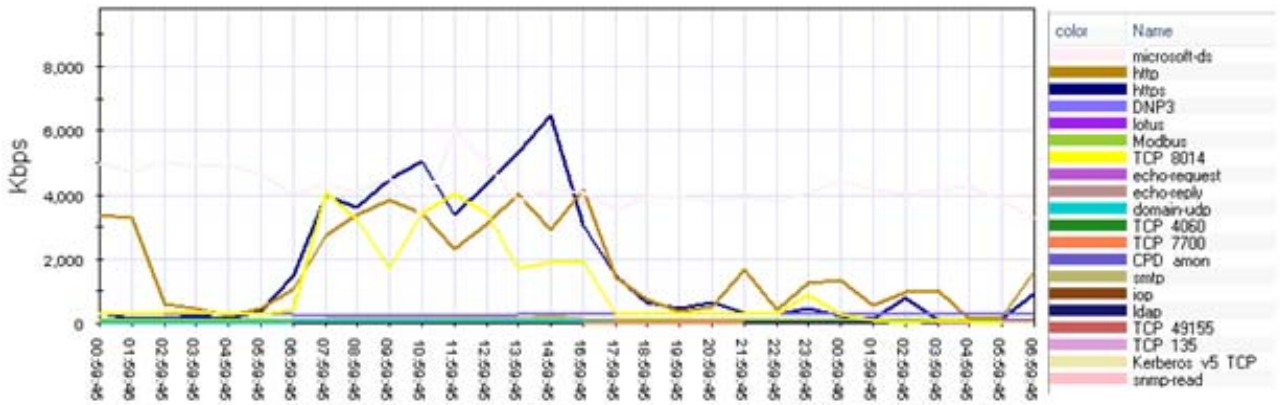
En el caso de la Figura 3.33, el tráfico que presenta mayor consumo es el protocolo HTTPS el cual presenta como máximo 7 MB cerca de alcanzar los 8 MB del ancho de banda para el Internet.

Figura 3. 33 Tipo de Tráfico - Del miércoles 3 al jueves 4 de Junio 2015



En el caso de la Figura 3.34, el tráfico que presenta mayor consumo es el protocolo HTTPS el cual presenta como máximo 6.5 MB cerca de alcanzar los 8 MB del ancho de banda para el Internet.

Figura 3. 34 Tipo de Tráfico - Del jueves 4 al viernes 5 de Junio 2015



En el caso de la Figura 3.35 y 3.36, el tráfico que presenta mayor consumo es el protocolo MICROSOFT-DS el cual presenta como máximo 4 MB. Es importante identificar que por ser fin de semana el tráfico se disminuye considerablemente, en especial el protocolo HTTP y HTTPS.

Figura 3. 35 Tipo de Tráfico - Del viernes 5 al sábado 6 de Junio 2015

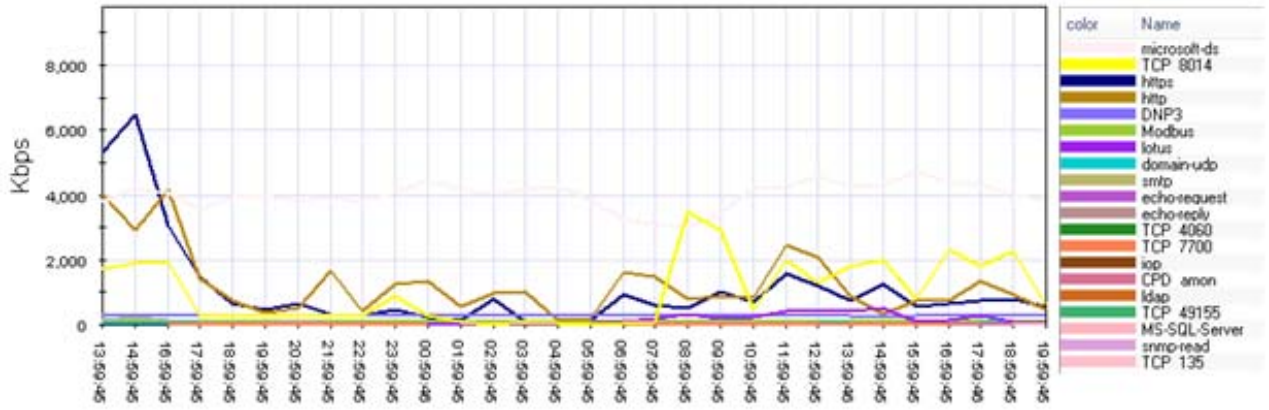
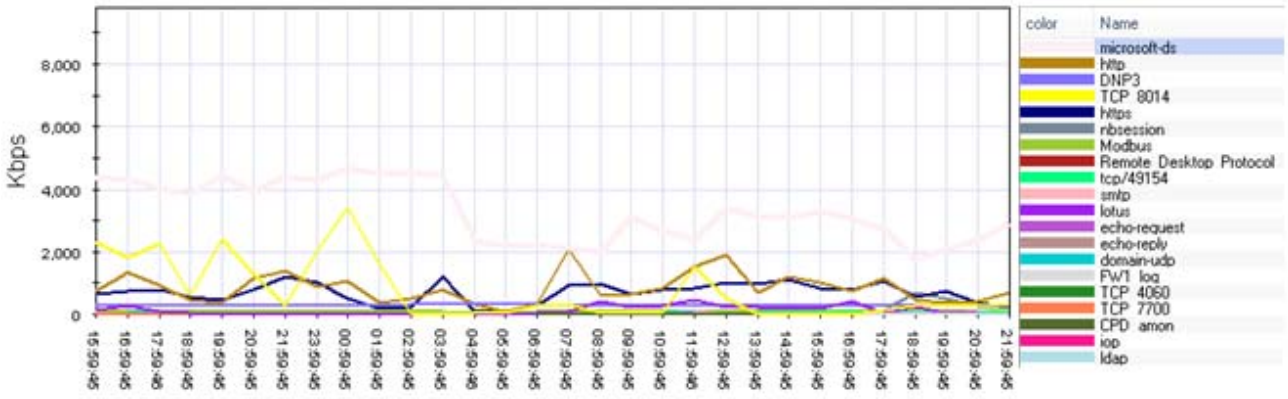
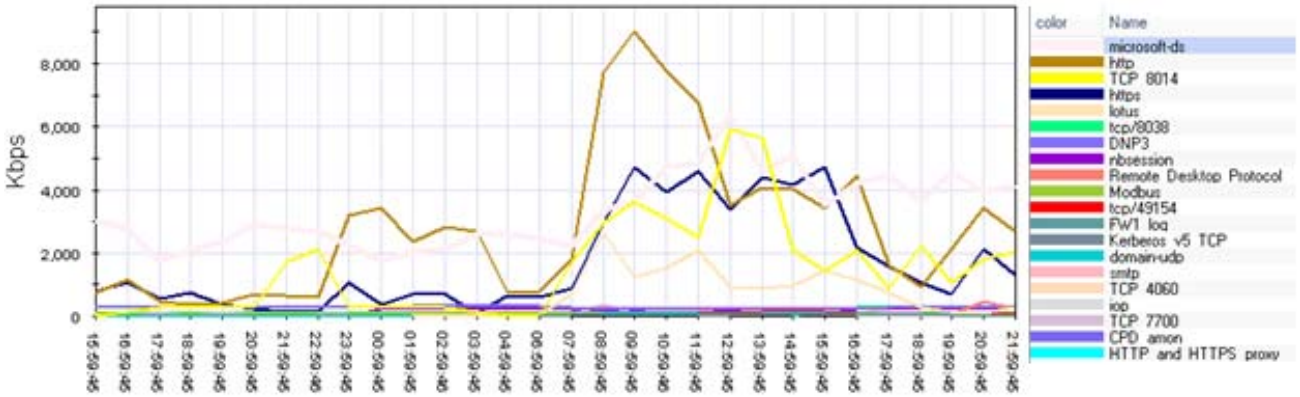


Figura 3. 36 Tipo de Tráfico - Del sábado 6 al domingo 7 de Junio 2015



En el caso de la Figura 3.37, el tráfico que presenta mayor consumo es el protocolo HTTPS el cual supera los 8 MB provocando una saturación del canal ya que el ancho de banda en cuanto a internet es de 8 MB para toda la Unidad de Negocios Termopichincha. Debido a que es el primer día de la semana el tráfico aumenta considerablemente.

Figura 3. 37 Tipo de Tráfico - Del domingo 7 al lunes 8 de Junio 2015



Como se puede evidenciar en las diferentes figuras el tipo de tráfico que genera mayor consumo es HTTP, HTTPS y MICROSOFT-DS, y en especial el primer día de la semana en donde el crecimiento del tráfico es alto. Los servicios de red mantenidos dentro de la Unidad de Negocios Termopichincha también son reflejados en las diferentes figuras.

3.5.2 Protocolos

Mediante la utilización del mecanismo NBAR se pudo obtener los protocolos que circulan en los diferentes routers dentro de la infraestructura de red de la Unidad de Negocios Termopichincha durante el mes de Mayo 2015. Las tablas 3.6, 3.7 y 3.8 muestran la información obtenida más relevante.

Tabla 3. 6 Datos NBAR Routerfw hacia CELEC

	Input	**Output**
Protocolo	Packet Count	Packet Count
ftp	11073161	22532793
http	18065906	14321724
cifs	69491996	41831263

binary-over-http	32411060	20628865
ssl	15485128	10284406
notes	7653082	7051497
imap	1582651	1817162
video-over-http	35505	58675
dns	2161800	1561381
smtp	618780	298975
rtmp	675629	385987
rtp	6923396	6876449
dnp	23507607	26939500
pop3	11357	8272
sqlserver	13710	19690
exchange	5272	4546
oracle-sqlnet	8784	14717
active-directory	282651	289736
ldap	106029	99238
webex-meeting	12031	13472
ping	354818	393772
snmp	337755	560776
icmp	54210	136873
telnet	14416	22066
rtmpt	84	52
sip	397	2861
h323	3775	3697
rtcp	26444	27093

Tabla 3. 7 Datos NBAR Router Quito hacia Guangopolo

	Input	Output
Protocol	Packet Count	Packet Count
http	23125099	45478565
ssl	23487852	18315633
cifs	5133852	74547279
notes	8246251	8812203
rtcp	125052	351867
video-over-http	169882	94847
secure-http	356037	331323
imap	1952407	1522408
smtp	291913	1025706
rtp	6928217	6980498
rtmp	1754390	961002
dnp	26227914	22059473
dns	1797537	2036049
pop3	2113	1422
ldap	105697	111992
active-directory	290915	284647
ftp	11	223209
webex-meeting	11586	13804
oracle-sqlnet	2932	8784
sqlserver	91	13540
snmp	32097	564060
ping	335718	464109

icmp	104510	8277
sip	30225	30208
h323	4921	5030

Tabla 3. 8 Datos NBAR Router Guangopolo hacia Quito

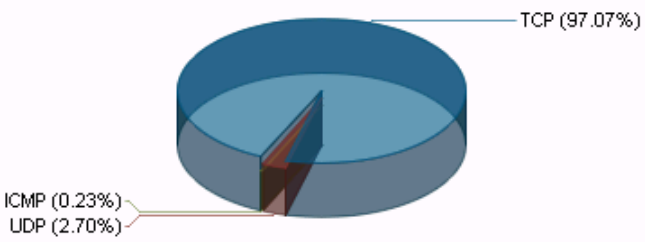
	Input	**Output**
Protocol	Packet Count	Packet Count
http	43237559	22069982
secure-http	24695046	29431189
microsoftds	61440152	48506
cifs	13011288	5092666
skype	300045	480261
imap	1693145	2039017
smtp	596120	282324
ftp-data	10737886	0
notes	90697	31295
h323	310638	253826
dns	1417970	1223705
netbios	902866	49423
exchange	929575	1205492
rtp	11553	9267
icmp	1417901	463234
pop3	1236	1963
ldap	188504	189726
secure-imap	76376	77476

ftp	224483	79
rtcp	3240	2944
sqlnet	18317	5180
snmp	1364048	832067
telnet	3228	2555
sqlserver	13954	6
sip	8944	8945
ntp	57830	11222

El porcentaje mayor de tráfico generado dentro de la Unidad de Negocios Termopichincha corresponde al protocolo TCP con un 97% , seguido del tráfico generado correspondiente al protocolo UDP con un 2.7% y por último el tráfico generado correspondiente al protocolo ICMP con un 0.2%.

Es importante recalcar que el mayor porcentaje corresponde a un protocolo TCP que garantiza que los datos sean entregados a su destino sin errores y que permite que las aplicaciones puedan comunicarse de manera segura. El protocolo ICMP corresponde a los sistemas de monitoreo implementados dentro de la infraestructura de red .

Figura 3. 38 Porcentajes de tráfico por protocolos



Protocol	Bytes	Rate	Utilization	Percentage
TCP	786.34 GB	8.71 Mbps	N/A	95.81 %
UDP	21.88 GB	242.30 Kbps	N/A	2.67 %
ICMP	1.84 GB	20.36 Kbps	N/A	0.22 %
Totals	810.06 GB	8.97 Mbps	N/A	98.7 %

3.5.3 Puertos

Mediante la utilización del monitoreo de Checkpoint se pudo obtener los distintos puertos que circulan dentro de la infraestructura de red de la Unidad de Negocios Termopichincha durante el mes de Mayo 2015. Claro está, que los protocolos ya identificados anteriormente poseen puertos específicos para comunicarse pero en la Figura 3.39 y 3.40 se muestran los puertos TCP y UDP utilizados por otros servicios.

Figura 3. 39 Puertos TCP

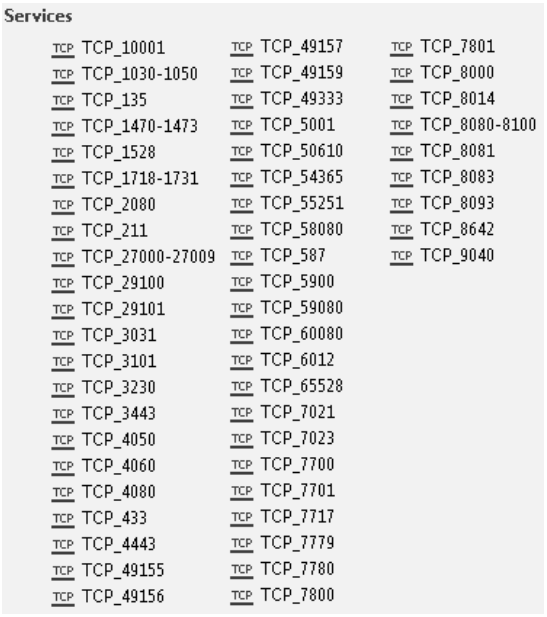
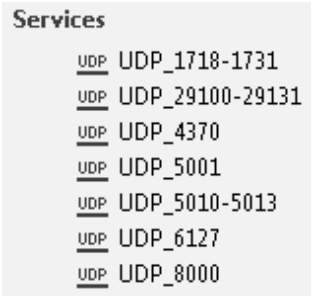


Figura 3. 40 Puertos UDP



3.5.4 Protocolos y Puertos de los Servicios de Red

Tomando en cuenta los servicios de red de la Unidad de Negocios Termopichincha y los datos obtenidos en los monitoreo de la infraestructura de red, las tablas 3.9 hasta la 3.15 muestran los protocolos y puertos utilizados actualmente para cada uno de los servicios.

Tabla 3. 9 IFS Protocolo y Puerto

Servicios de Red	Protocolo	Puerto
IFS (Sistema Financiero Integrado)	TCP	58080
		59080
		60080
		8093
	microsoft-ds	445
	nbname	137
	nbsession	139
	ftp	21

Tabla 3. 10 Videoconferencia Protocolo y Puerto

Servicios de Red	Protocolo	Puerto
Video Conferencia	H323	1720
	H323_ras	1719
	HTTP	80
	HTTPS	443
	SIP	5060
	TCP	1718 - 1731
		3230
		5001
	UDP	1718 - 1731
		5001

Tabla 3. 11 Telefonía Protocolo y Puerto

Servicios de Red	Protocolo	Puerto
Telefonía IP	H323	1720
	H323_ras	1719
	Multidropper	1035
	SIP	5060
	TCP	1030 - 1050
		1528
		29100
		29101
		4060
		8000
	UDP	29100 -29131
		5010 -5013
		8000

Tabla 3. 12 Correo Protocolo y Puerto

Servicios de Red	Protocolo	Puerto
Correo	imap	143
	imap-ssl	993
	lotus	1352
	pop-3	110
	smtp	25
	TCP	6012

Tabla 3. 13 Scada Protocolo y Puerto

Servicios de Red	Protocolo	Puerto
Scada	DNP3	20000
	HTTP	80
	ICMP	
	ModBus	502
	Telnet	23
	TCP	10001
		4050
		7700
		7701
		7717
		7779
		7800
		7801
		433
		50610
		49333

Tabla 3. 14 Lotus Protocolo y Puerto

Servicios de Red	Protocolo	Puerto
Lotus	HTTP	80
	HTTPS	443
	lotus	1352
	Sametime	1533
	microsoft-ds	445
	nbname	137
	nbsession	139

Tabla 3. 15 Otros servicios de red con su respectivo protocolo y puerto

Servicios de Red	Protocolo	Puerto
Dominio	ntp	123
	domain-tcp	53
	Kerberos_v5	88
	ldap	389
	microsoft-ds	445
	nbname	137
	nbsession	139
	nbdatagram	138
	TCP	135
		49155
		49156
		49157
		49159

Evolution	HTTP	80
Base de Datos	MS-SQL-Server	1433
	MS-SQL-Monitor	1434
Antivirus	TCP	8014
Autocad	TCP	2080
		27000 - 27009

3.5.5 Ancho de Banda

Mediante la utilización de la herramienta WhastUp se ha procedido con la medición del ancho de banda en cada uno de los equipos switchs de comunicación dentro de la red LAN y routers en la red WAN, en un periodo de 1 semana las 24 horas del día.

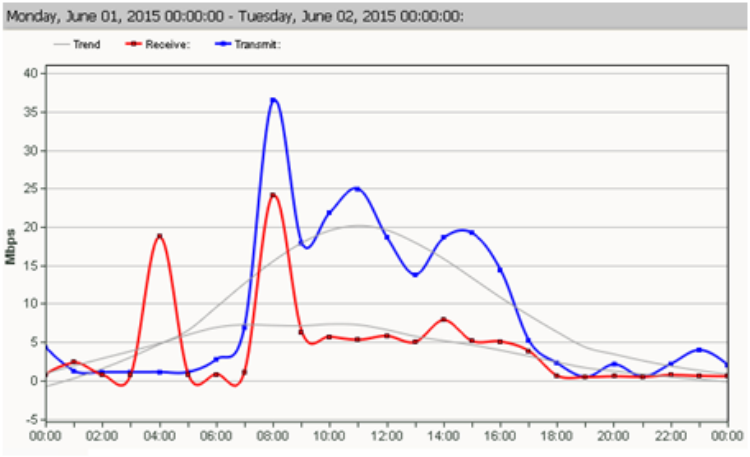
En el caso de los enlaces de la red LAN, se han monitoreado las interfaces configuradas como trunk en cada switch y que forman la topología en anillo. Las siguientes figuras muestran el consumo generado de cada uno de los enlaces, identificando el color rojo como la Recepción y color azul como la Transmisión.

3.5.5.1 Enlace CORE - SWDATACENTER

Los porcentajes de mayor consumo son reportados dentro de las horas de oficina, que comprende desde las 8:00 hasta 17:00, con un consumo máximo de transmisión de 51.5 Mbps y un máximo de recepción de 43 Mbps. Las figuras 3.41, 3.42, 3.43, 3.44 y 3.47 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 de cada día, en donde se puede evidenciar que los valores de transmisión y recepción varían durante las horas de oficina con picos altos durante las primeras horas de la mañana. Adicionalmente se presenta una variación en la recepción durante las 4:00 debido a un proceso automatizado de respaldos. Las figuras 3.45 y

3.46 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 durante el fin de semana, en donde se puede evidenciar que los valores de transmisión y recepción son menores con variaciones mínimas. Adicionalmente se puede observar la variación en la recepción durante las 4:00 debido al mismo proceso automatizado de respaldos. La figura 3.48 muestra el monitoreo realizado durante toda la semana, en donde se puede evidenciar el alto consumo durante el día Lunes.

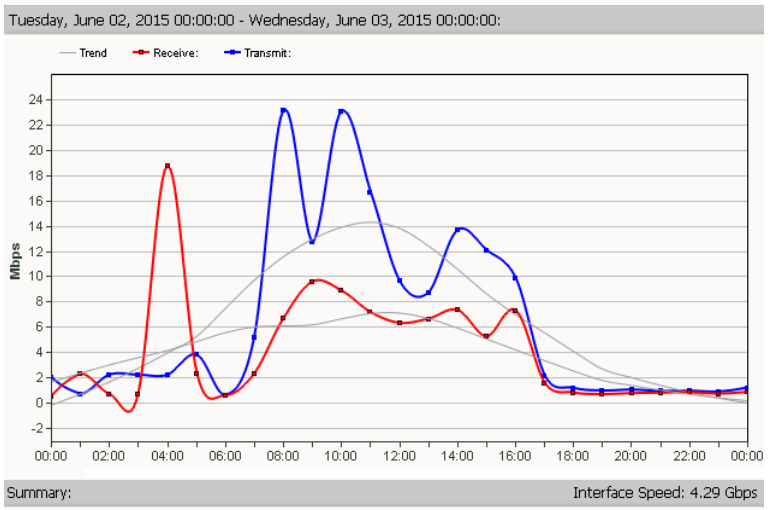
Figura 3. 41 Consumo de ancho de banda lunes 01 al martes 02 de Junio



Summary: Interface Speed: 4.29 Gbps

	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	400.69 Kbps	40.09 Mbps	4.15 Mbps	0.01 %	0.93 %	0.1 %
Transmit:	389.98 Kbps	51.45 Mbps	8.91 Mbps	0.01 %	1.2 %	0.21 %

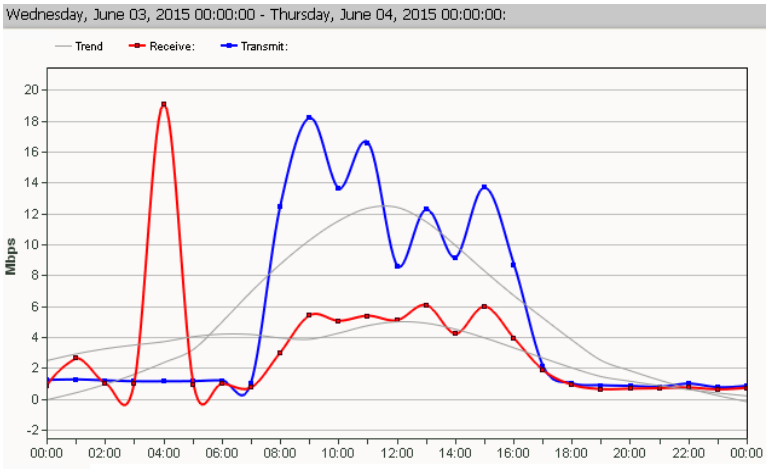
Figura 3. 42 Consumo de ancho de banda martes 02 al miércoles 03 de Junio



Summary: Interface Speed: 4.29 Gbps

	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	406.69 Kbps	42.47 Mbps	4.00 Mbps	**0.01 %**	**0.99 %**	**0.09 %**
Transmit:	389.98 Kbps	34.22 Mbps	6.20 Mbps	**0.01 %**	**0.8 %**	**0.14 %**

Figura 3. 43 Consumo de ancho de banda miércoles 03 al jueves 04 de Junio



Summary: Interface Speed: 4.29 Gbps

	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	527.70 Kbps	40.67 Mbps	3.12 Mbps	**0.01 %**	**0.95 %**	**0.07 %**
Transmit	629.58 Kbps	27.15 Mbps	5.21 Mbps	**0.01 %**	**0.63 %**	**0.12 %**

Figura 3. 44 Consumo de ancho de banda jueves 04 al viernes 05 de Junio

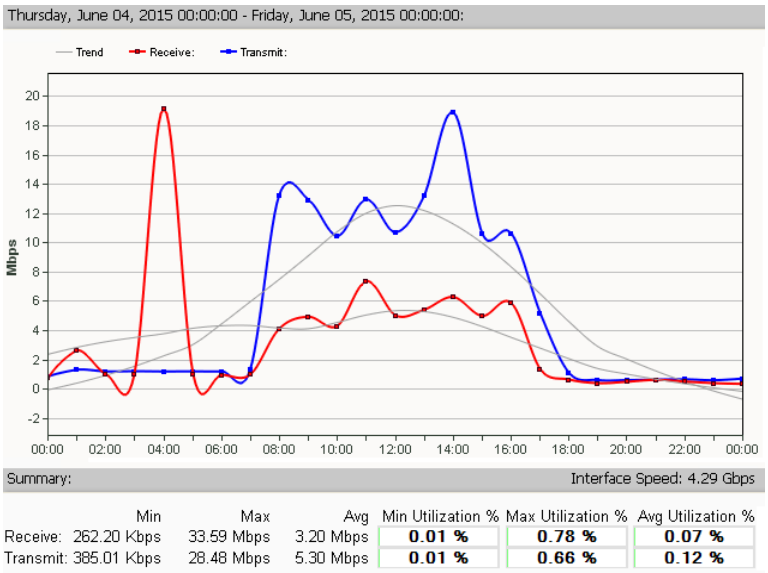


Figura 3. 45 Consumo de ancho de banda sábado 06 al domingo 07 de Junio

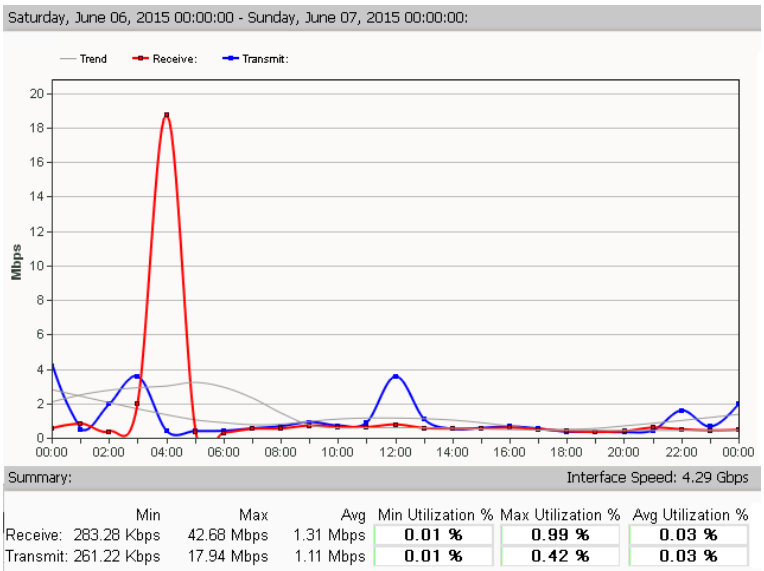
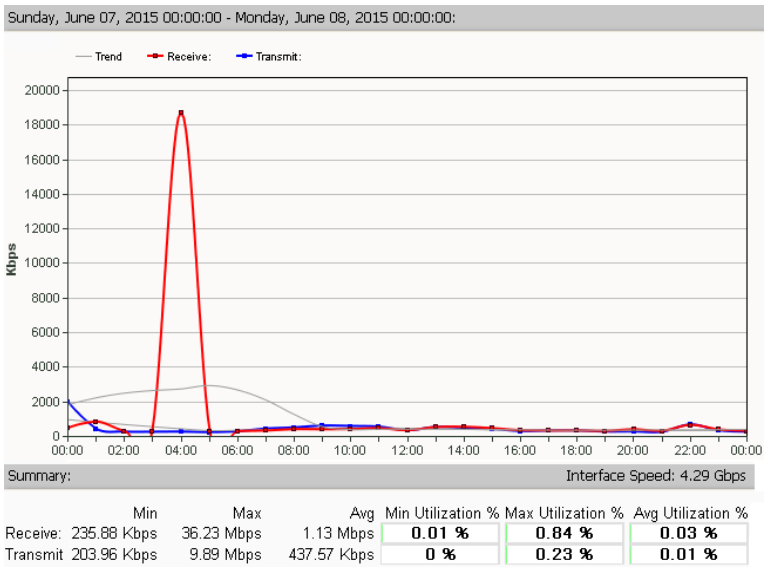
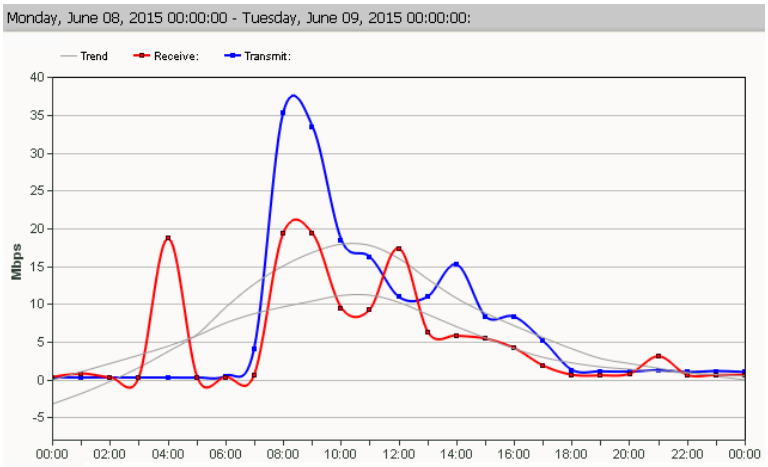


Figura 3. 46 Consumo de ancho de banda domingo 07 al lunes 08 de Junio



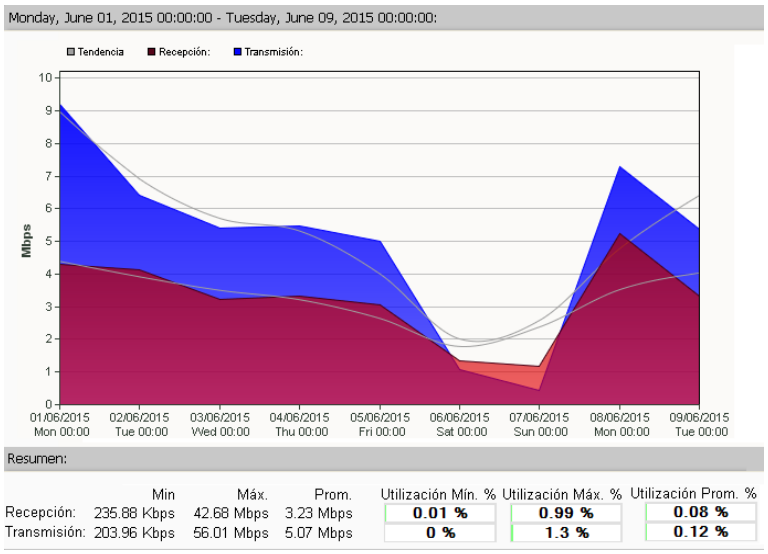
	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	235.88 Kbps	36.23 Mbps	1.13 Mbps	0.01 %	0.84 %	0.03 %
Transmit	203.96 Kbps	9.89 Mbps	437.57 Kbps	0 %	0.23 %	0.01 %

Figura 3. 47 Consumo de ancho de banda lunes 08 al martes 09 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	252.26 Kbps	37.18 Mbps	5.06 Mbps	0.01 %	0.87 %	0.12 %
Transmit:	218.71 Kbps	56.01 Mbps	7.03 Mbps	0.01 %	1.3 %	0.16 %

Figura 3. 48 Consumo de ancho de banda de la semana del lunes 01 al martes 09 de Junio



3.5.5.2 Enlace CORE - SWTECNICA

Los porcentajes de mayor consumo son reportados dentro de las horas de oficina, que comprende desde las 8:00 hasta 17:00, con un consumo máximo de transmisión de 56.7 Mbps un máximo de recepción de 31.8 Mbps. Las figuras 3.49, 3.50, 3.51, 3.52 y 3.55 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 de cada día, en donde se puede evidenciar que los valores de transmisión y recepción varían durante las horas de oficina con picos altos durante las primeras horas de la mañana. Las figuras 3.53 y 3.54 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 durante el fin de semana, en donde se puede evidenciar que los valores de transmisión y recepción son menores con variaciones mínimas. La figura 3.56 muestra el monitoreo realizado durante toda la semana, en donde se puede evidenciar el alto consumo durante el día Lunes.

Figura 3. 49 Consumo de ancho de banda lunes 01 al martes 02 de Junio

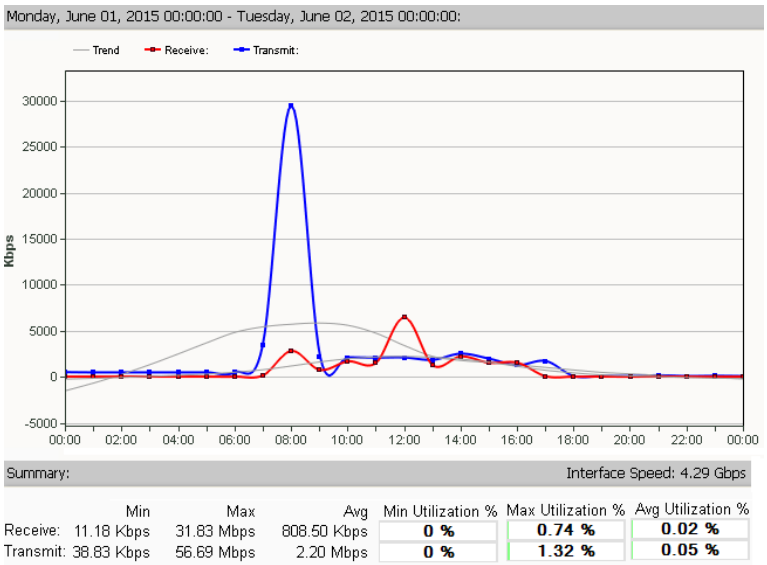


Figura 3. 50 Consumo de ancho de banda martes 02 al miércoles 03 de Junio

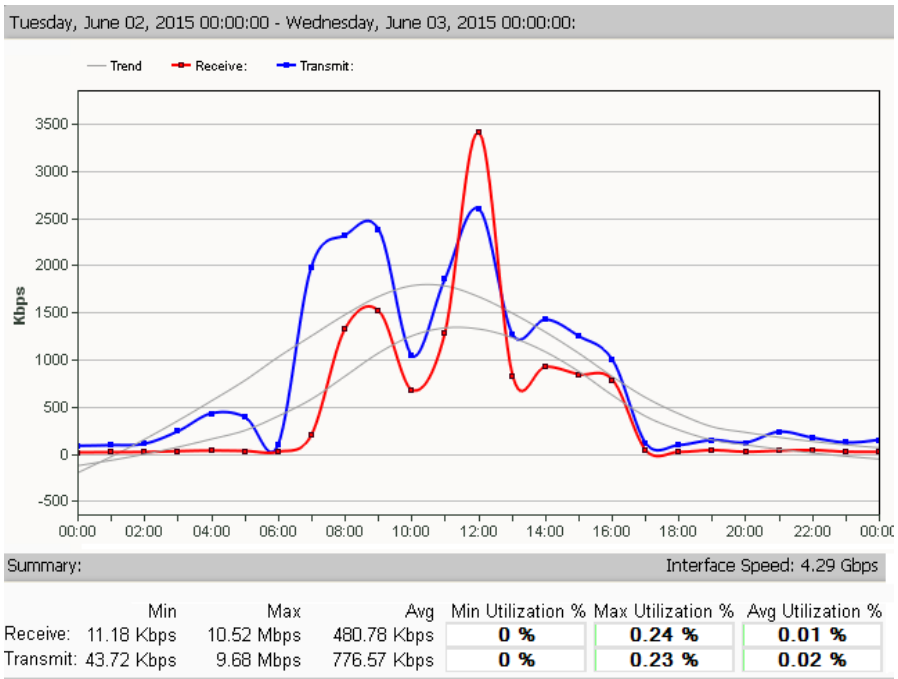
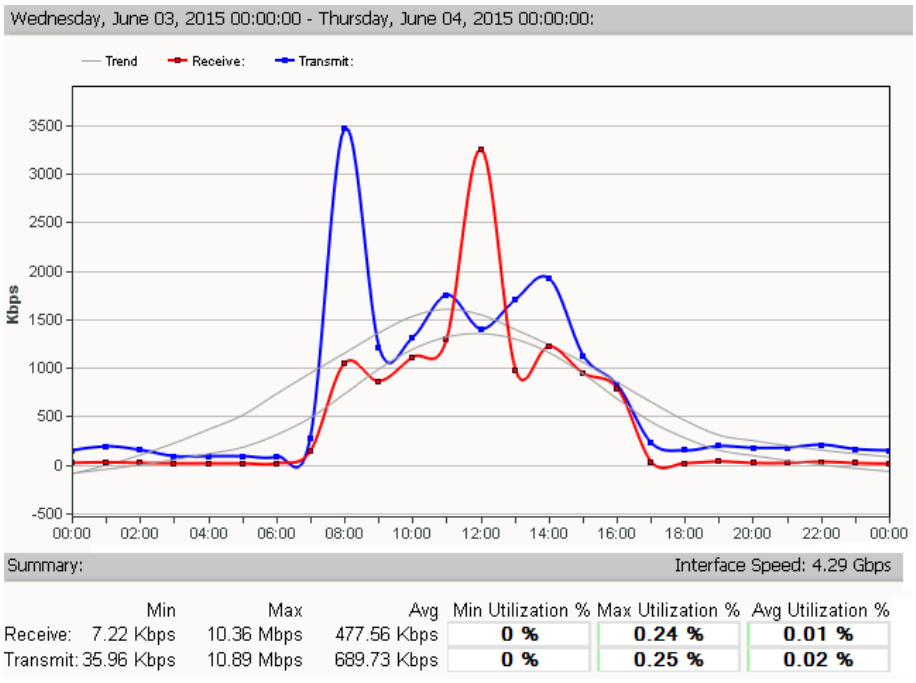
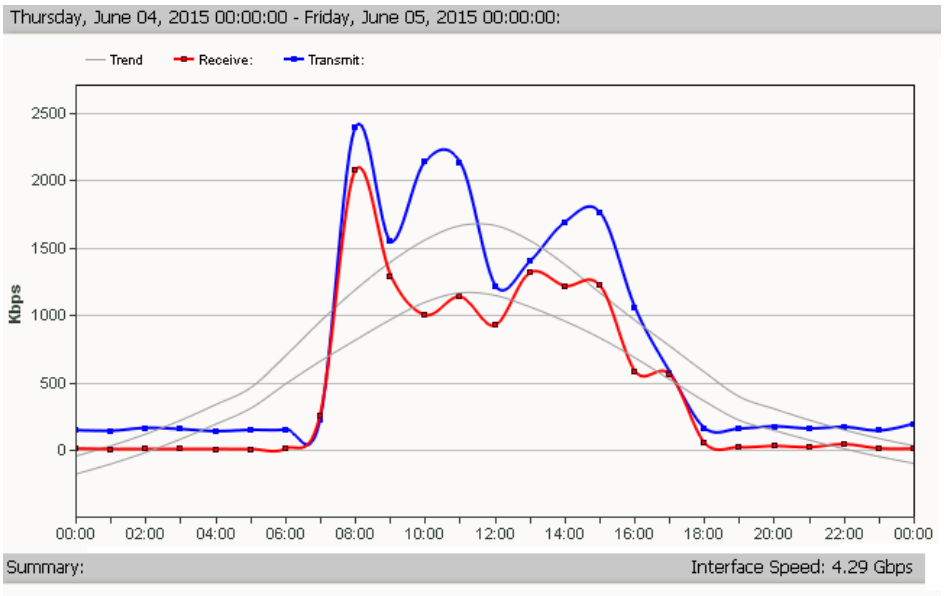


Figura 3. 51 Consumo de ancho de banda miércoles 03 al jueves 04 de Junio



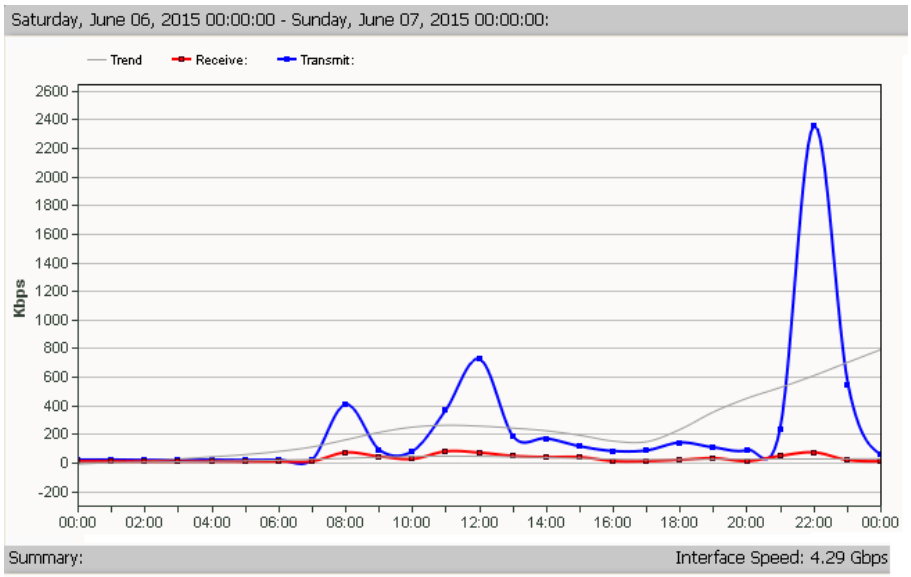
	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	7.22 Kbps	10.36 Mbps	477.56 Kbps	0 %	0.24 %	0.01 %
Transmit:	35.96 Kbps	10.89 Mbps	689.73 Kbps	0 %	0.25 %	0.02 %

Figura 3. 52 Consumo de ancho de banda jueves 04 al viernes 05 de Junio



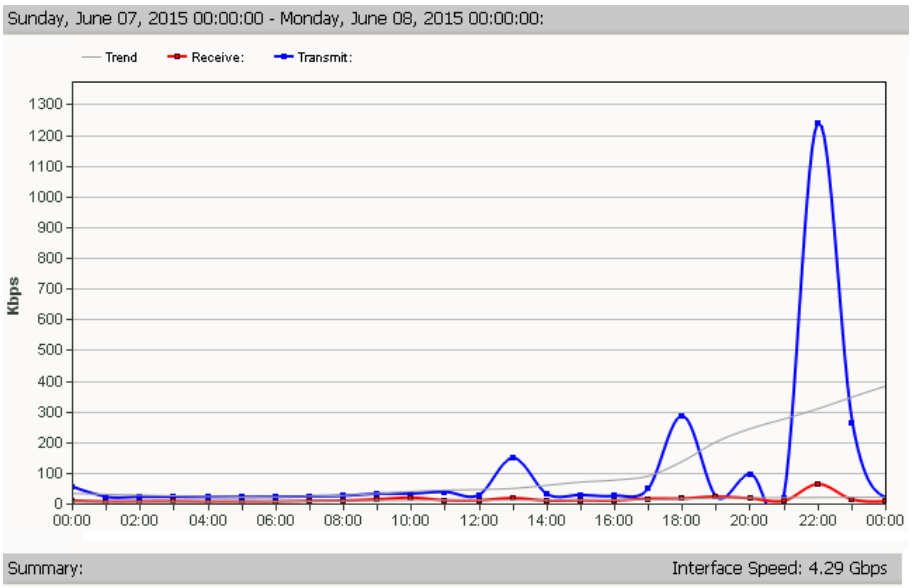
	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	6.44 Kbps	7.10 Mbps	474.29 Kbps	0 %	0.17 %	0.01 %
Transmit	36.19 Kbps	3.61 Mbps	735.21 Kbps	0 %	0.08 %	0.02 %

Figura 3. 53 Consumo de ancho de banda sábado 06 al domingo 07 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	4.18 Kbps	274.54 Kbps	27.95 Kbps	0 %	0.01 %	0 %
Transmit:	17.30 Kbps	7.11 Mbps	238.86 Kbps	0 %	0.17 %	0.01 %

Figura 3. 54 Consumo de ancho de banda domingo 07 al lunes 08 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	4.11 Kbps	314.18 Kbps	13.12 Kbps	0 %	0.01 %	0 %
Transmit:	16.21 Kbps	7.27 Mbps	103.26 Kbps	0 %	0.17 %	0 %

Figura 3. 55 Consumo de ancho de banda lunes 08 al martes 09 de Junio

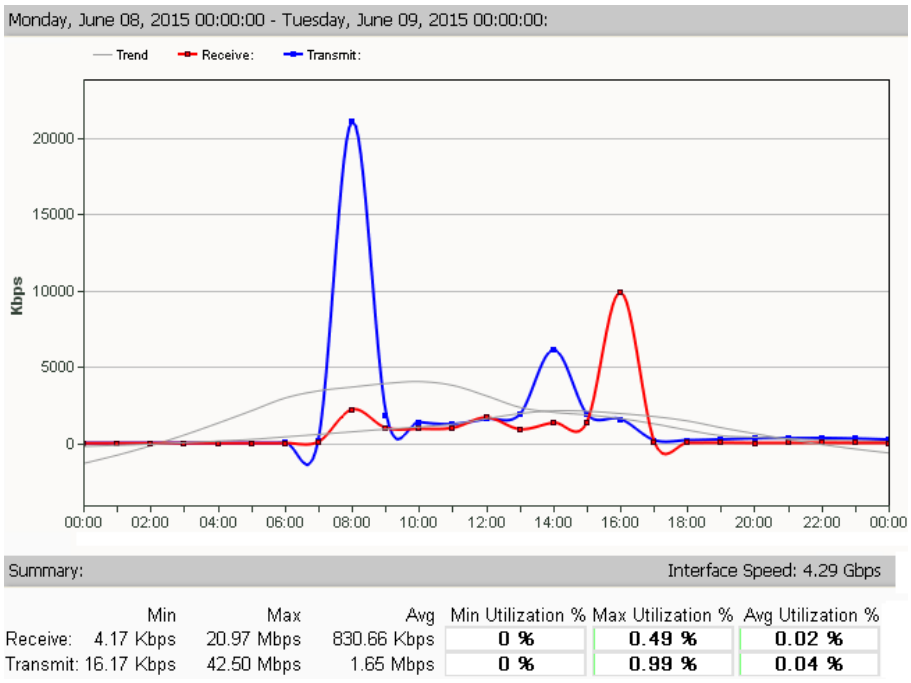
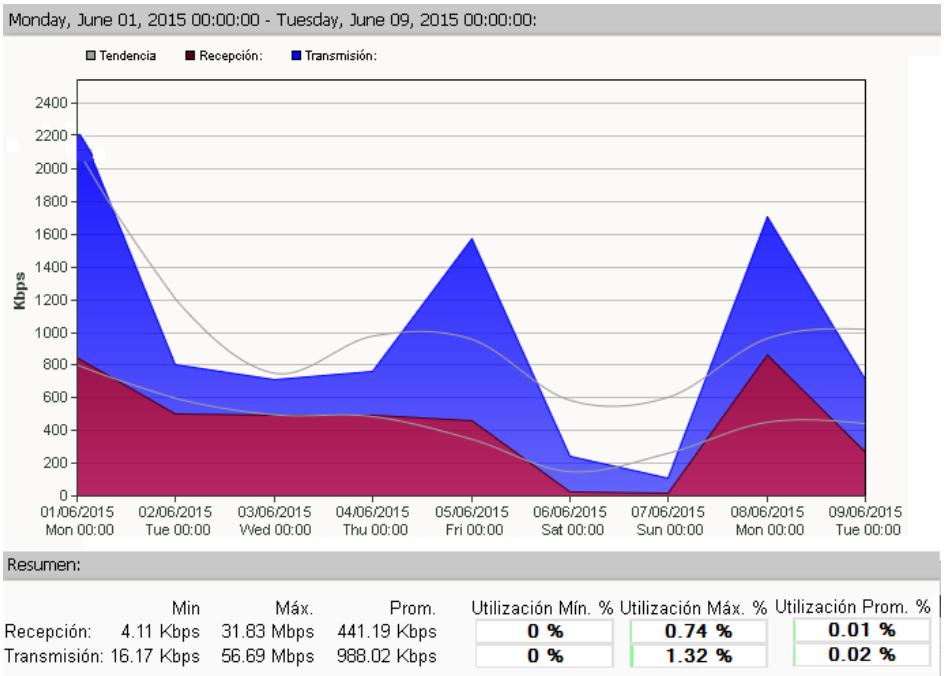


Figura 3. 56 Consumo de ancho de banda de la semana del lunes 01 al martes 09 de Junio



3.5.5.3 Enlace CORE - SWGUANGOPOLOII

Los porcentajes de mayor consumo no son reportados dentro de las horas de oficina, que comprende desde las 8:00 hasta 17:00, ya que este enlace es utilizado por la parte de operación, con un consumo máximo de transmisión de 10.3 Mbps y un máximo de recepción de 901 Kbps. Las figuras 3.57, 3.58, 3.59, 3.60 y 3.63 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 de cada día, en donde se puede evidenciar que los valores de transmisión y recepción varían durante todo el día debido a que es un enlace utilizado por personal operativo que trabaja las 24 horas del día. Las figuras 3.61 y 3.62 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 durante el fin de semana, en donde se puede evidenciar que los valores de transmisión y recepción son similares al tráfico de toda la semana. La figura 3.64 muestra el monitoreo realizado durante toda la semana, en donde se puede evidenciar el consumo diario.

Figura 3. 57 Consumo de ancho de banda lunes 01 al martes 02 de Junio

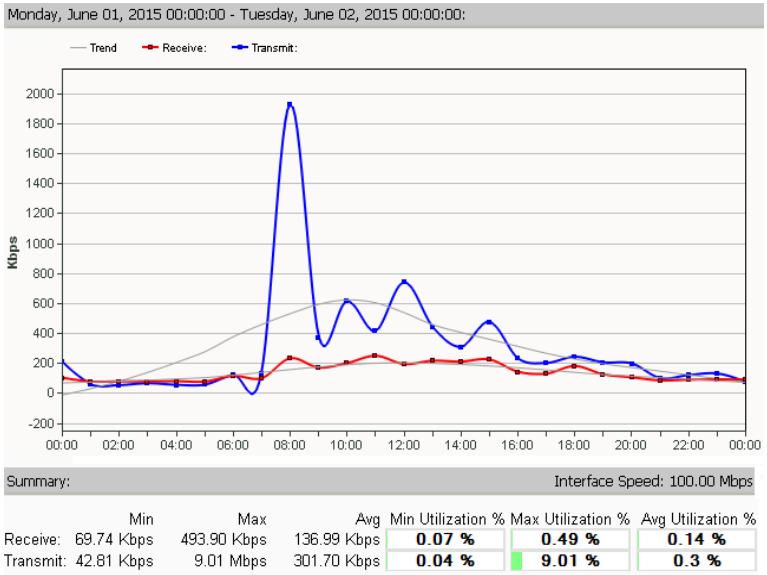


Figura 3. 58 Consumo de ancho de banda martes 02 al miércoles 03 de Junio

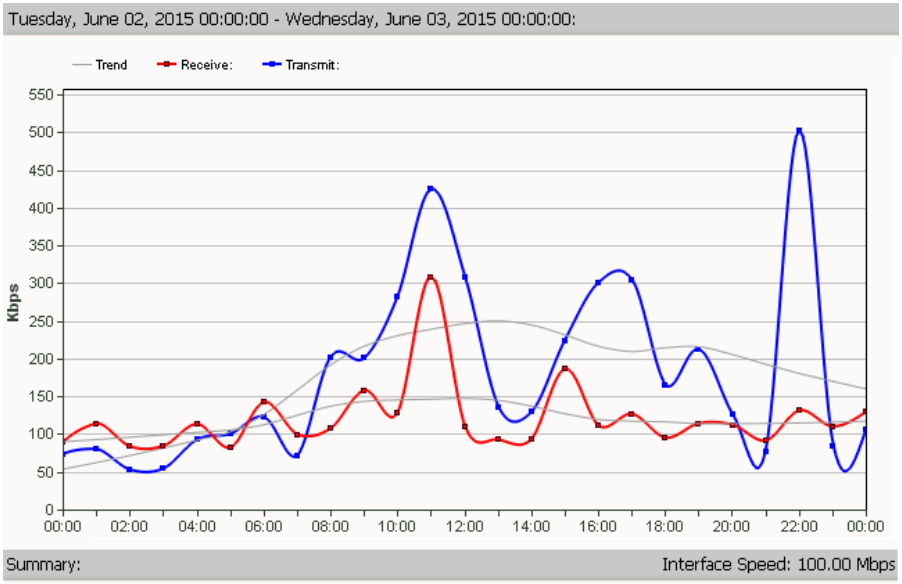


Figura 3. 59 Consumo de ancho de banda miércoles 03 al jueves 04 de Junio

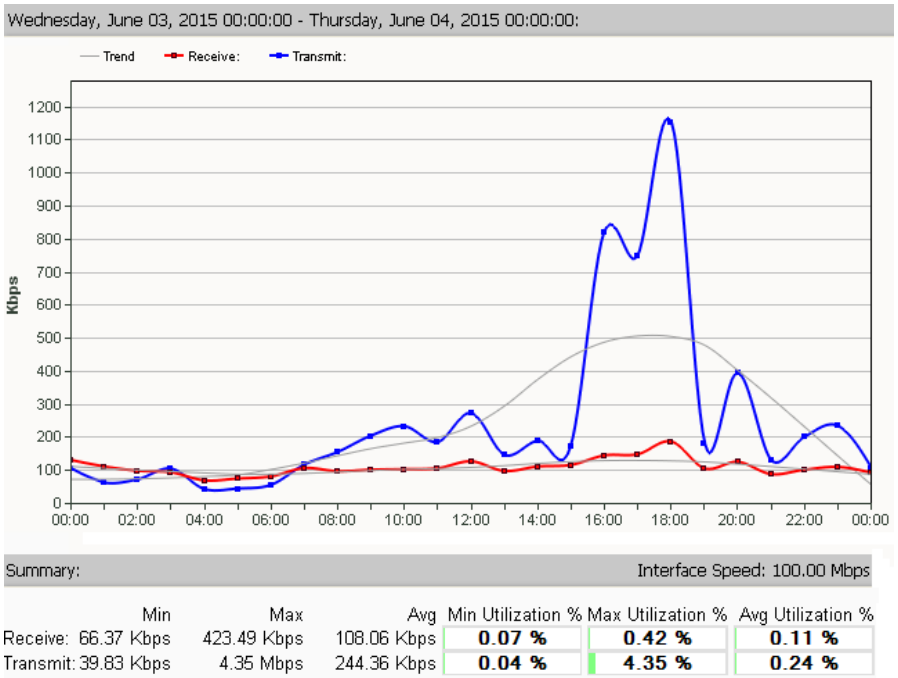


Figura 3. 60 Consumo de ancho de banda jueves 04 al viernes 05 de Junio

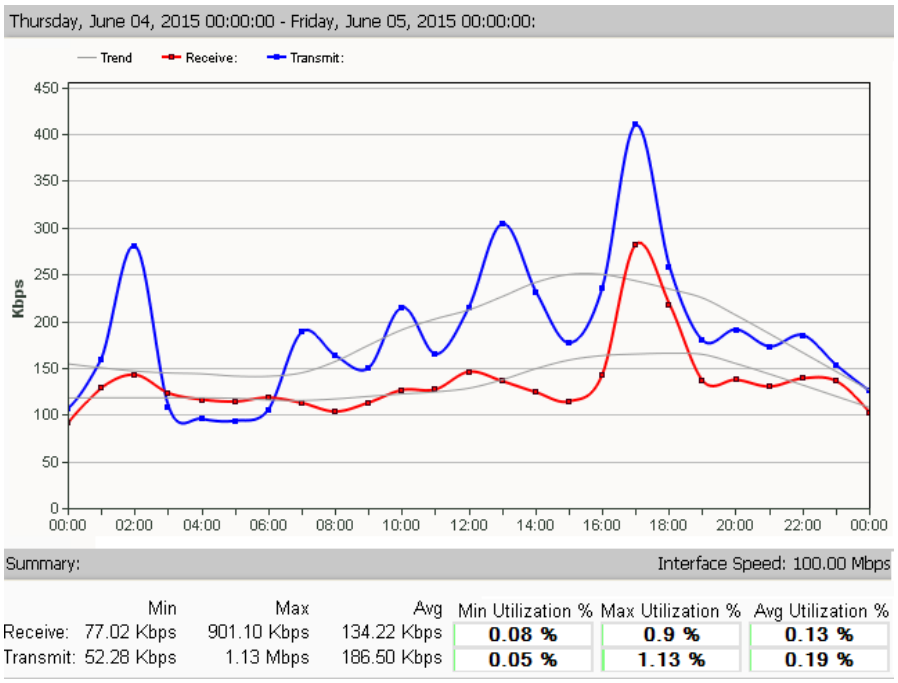


Figura 3. 61 Consumo de ancho de banda sábado 06 al domingo 07 de Junio

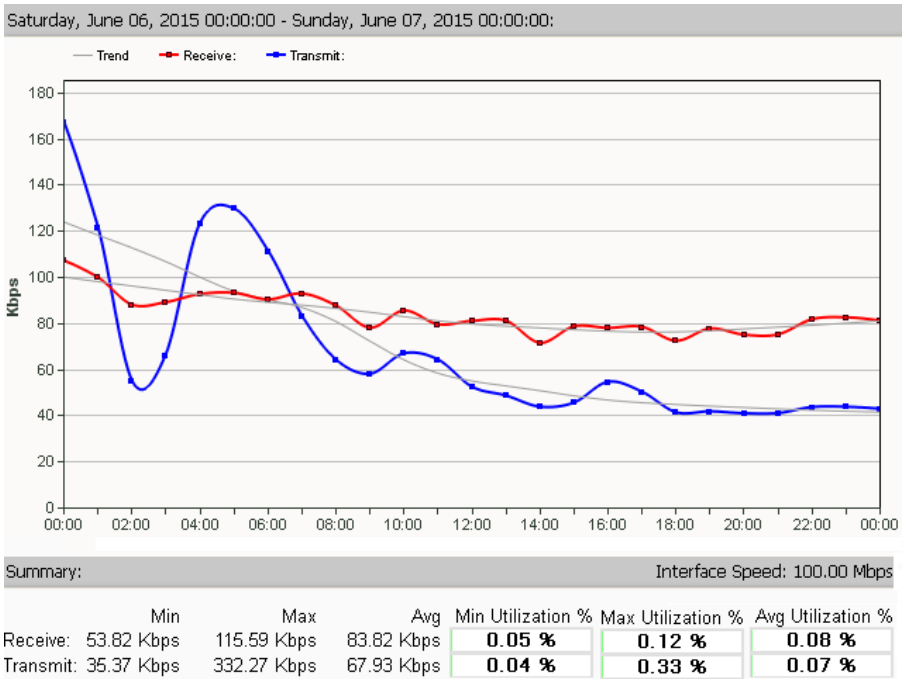


Figura 3. 62 Consumo de ancho de banda domingo 07 al lunes 08 de Junio

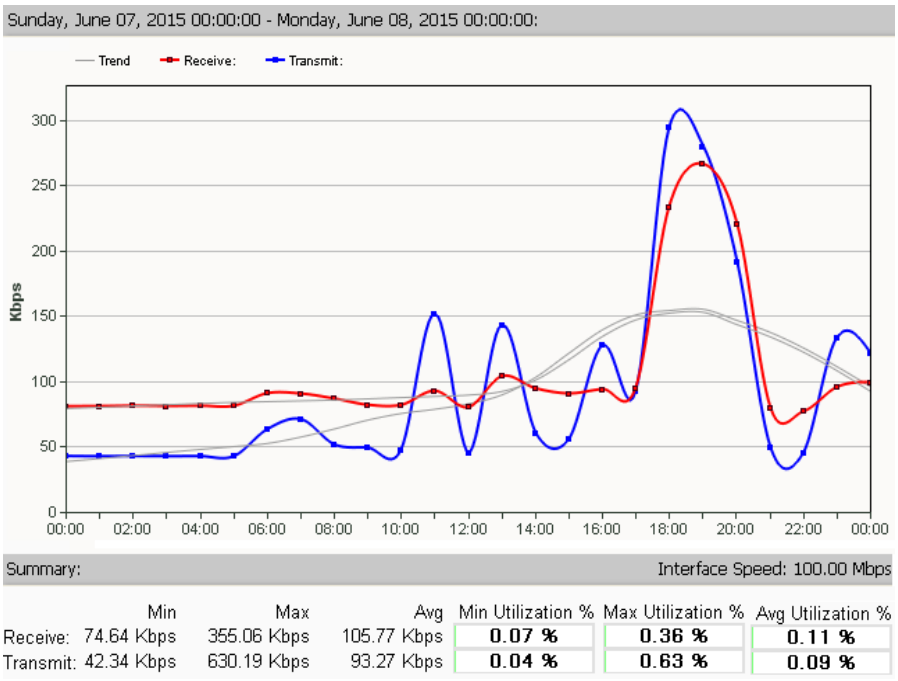


Figura 3. 63 Consumo de ancho de banda lunes 08 al martes 09 de Junio

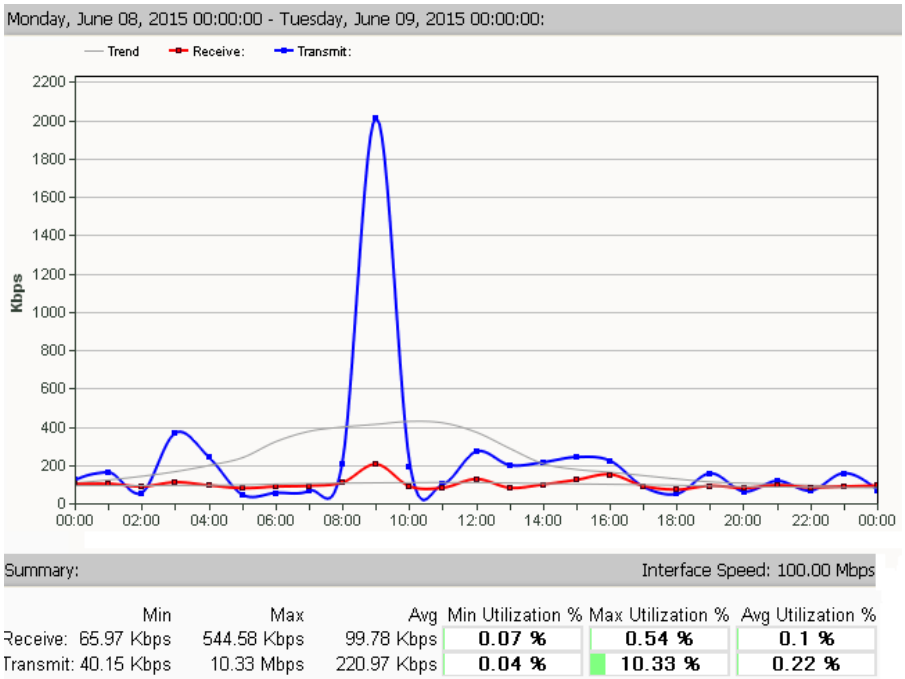
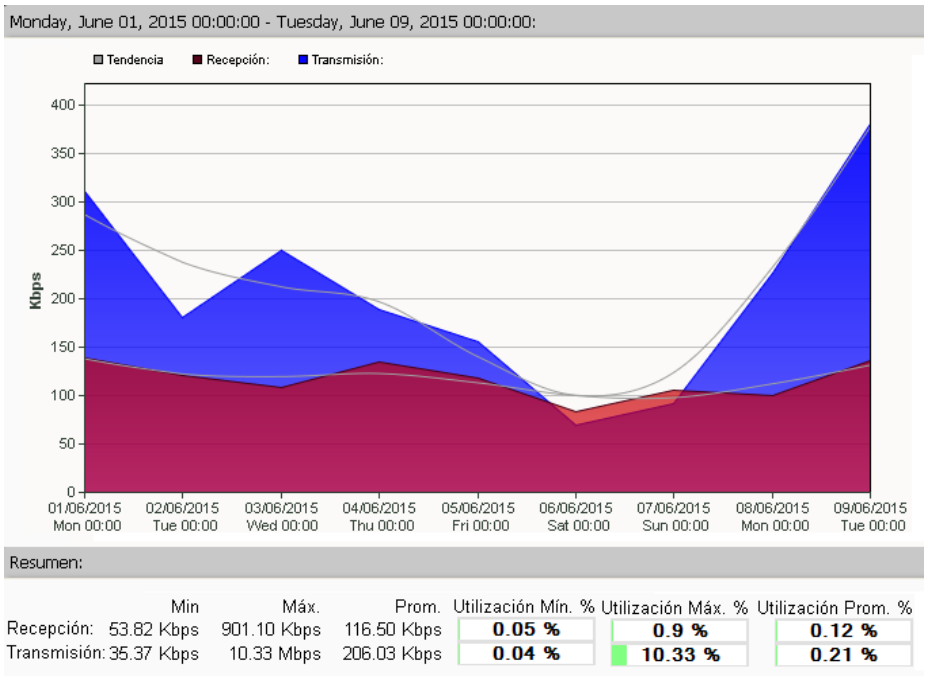


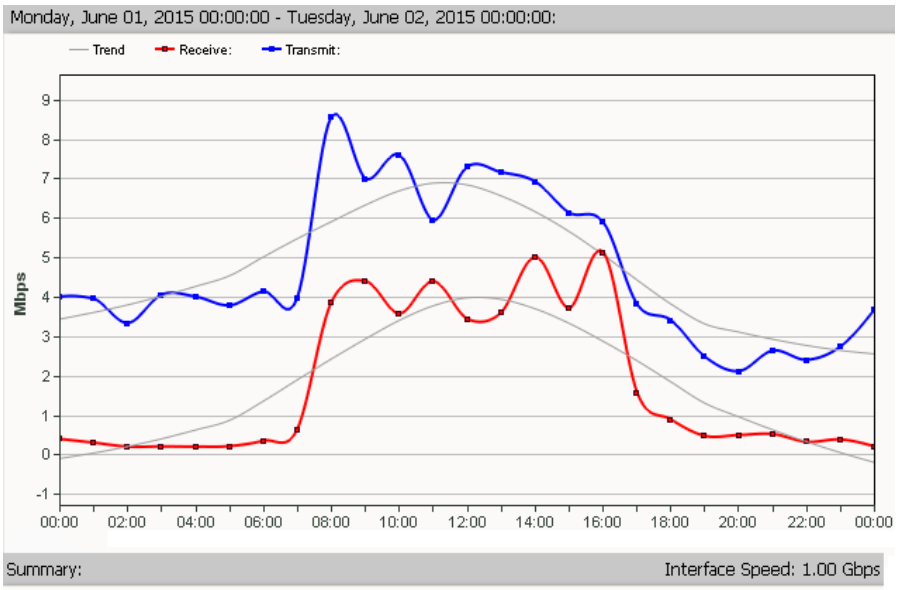
Figura 3. 64 Consumo de ancho de banda de la semana del lunes 01 al martes 09 de Junio



3.5.5.4 Enlace CORE - ROUTER GUANGOPOLO

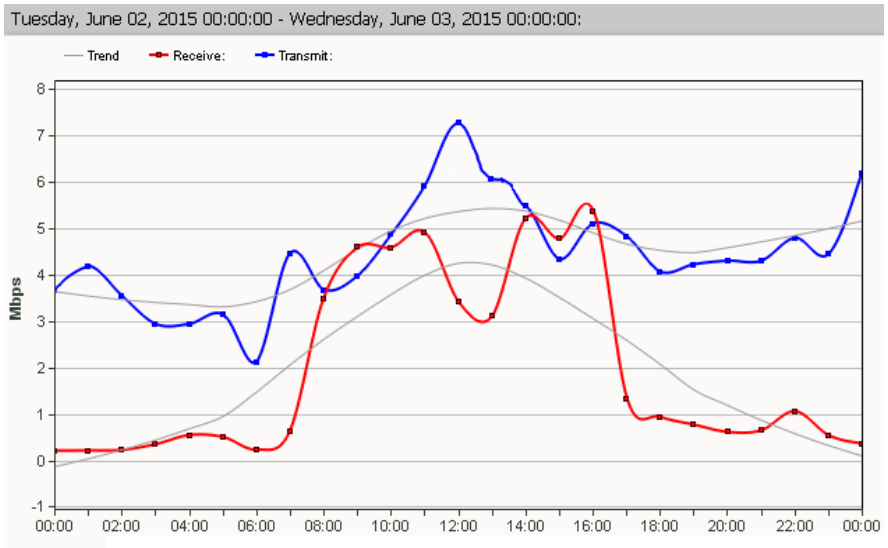
Los porcentajes de mayor consumo son reportados dentro de las horas de oficina, que comprende desde las 8:00 hasta 17:00, con un consumo máximo de transmisión de 12.6 Mbps y un máximo de recepción de 8.8 Mbps. Las figuras 3.65, 3.66, 3.67, 3.68 y 3.71 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 de cada día, en donde se puede evidenciar que los valores de transmisión y recepción varían durante todo el día pero con la característica de que la transmisión tiene mayor consumo. Las figuras 3.69 y 3.70 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 durante el fin de semana, en donde se puede evidenciar que los valores de transmisión y recepción presentan valores bajos. La figura 3.71 muestra el monitoreo realizado durante toda la semana, en donde se puede evidenciar el consumo diario.

Figura 3. 65 Consumo de ancho de banda lunes 01 al martes 02 de Junio



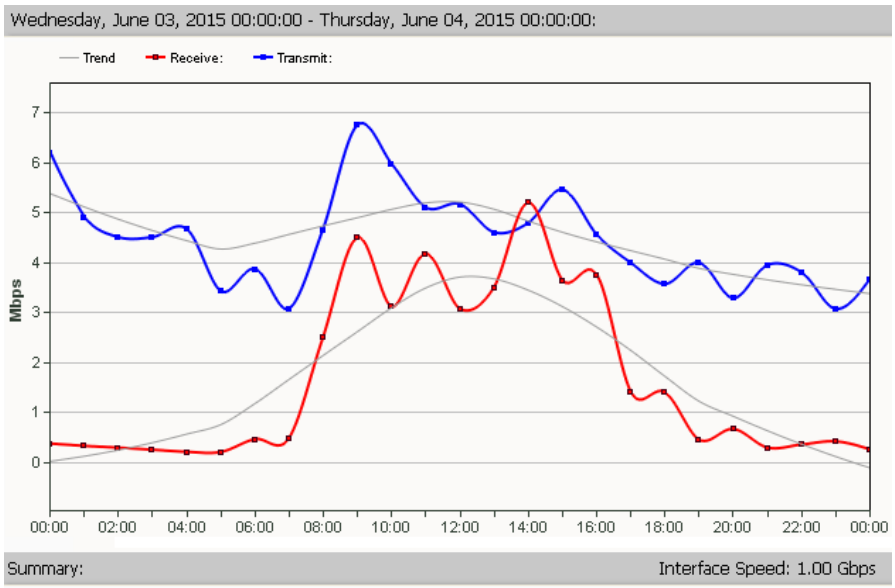
	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	172.78 Kbps	8.79 Mbps	1.76 Mbps	0.02 %	0.88 %	0.18 %
Transmit:	1.52 Mbps	12.65 Mbps	4.67 Mbps	0.15 %	1.26 %	0.47 %

Figura 3. 66 Consumo de ancho de banda martes 02 al miércoles 03 de Junio



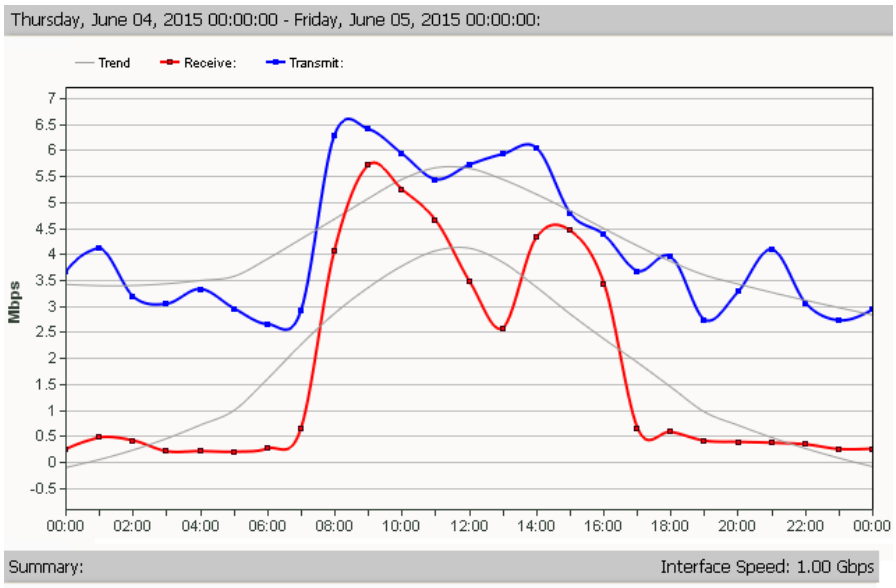
	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	172.78 Kbps	7.72 Mbps	1.93 Mbps	0.02 %	0.77 %	0.19 %
Transmit:	1.44 Mbps	7.75 Mbps	4.42 Mbps	0.14 %	0.77 %	0.44 %

Figura 3. 67 Consumo de ancho de banda miércoles 03 al jueves 04 de Junio



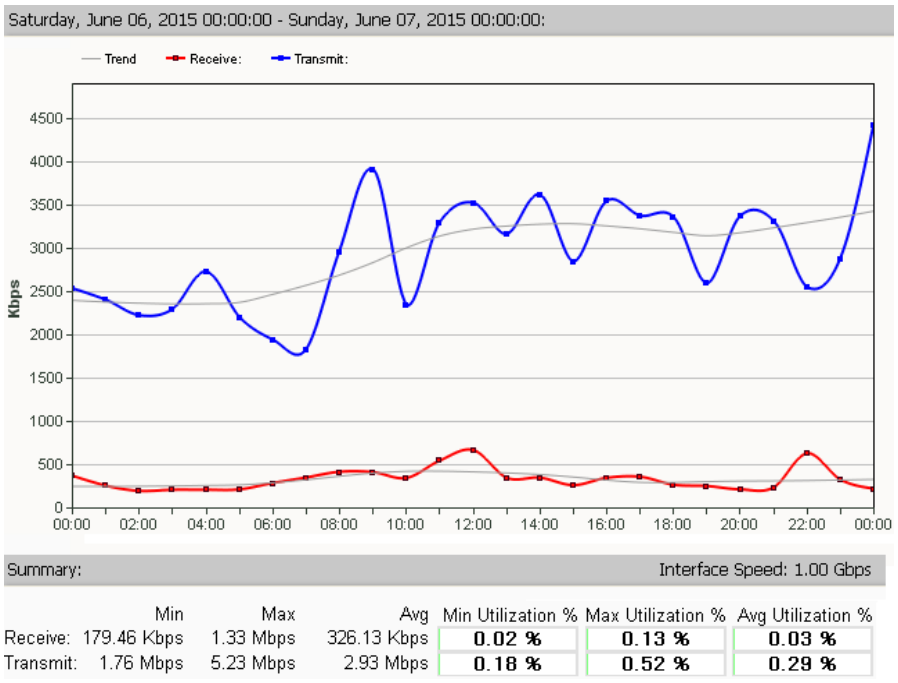
	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	180.98 Kbps	6.97 Mbps	1.64 Mbps	0.02 %	0.7 %	0.16 %
Transmit:	2.43 Mbps	8.11 Mbps	4.45 Mbps	0.24 %	0.81 %	0.45 %

Figura 3. 68 Consumo de ancho de banda jueves 04 al viernes 05 de Junio



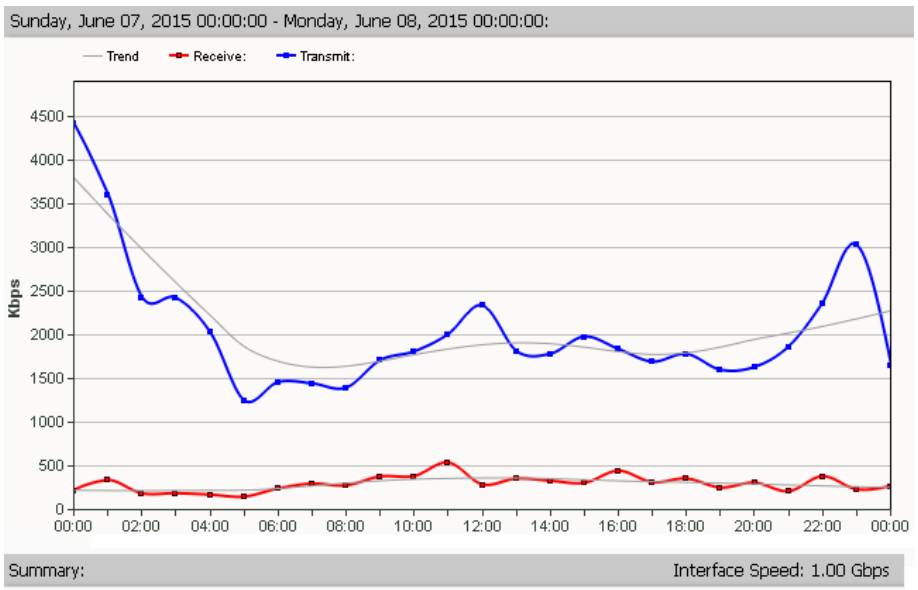
	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	184.72 Kbps	6.81 Mbps	1.75 Mbps	0.02 %	0.68 %	0.17 %
Transmit:	2.31 Mbps	9.56 Mbps	4.12 Mbps	0.23 %	0.96 %	0.41 %

Figura 3. 69 Consumo de ancho de banda sábado 06 al domingo 07 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	179.46 Kbps	1.33 Mbps	326.13 Kbps	0.02 %	0.13 %	0.03 %
Transmit:	1.76 Mbps	5.23 Mbps	2.93 Mbps	0.18 %	0.52 %	0.29 %

Figura 3. 70 Consumo de ancho de banda domingo 07 al lunes 08 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	133.06 Kbps	1.20 Mbps	289.97 Kbps	0.01 %	0.12 %	0.03 %
Transmit:	1.10 Mbps	5.23 Mbps	2.05 Mbps	0.11 %	0.52 %	0.2 %

Figura 3. 71 Consumo de ancho de banda lunes 08 al martes 09 de Junio

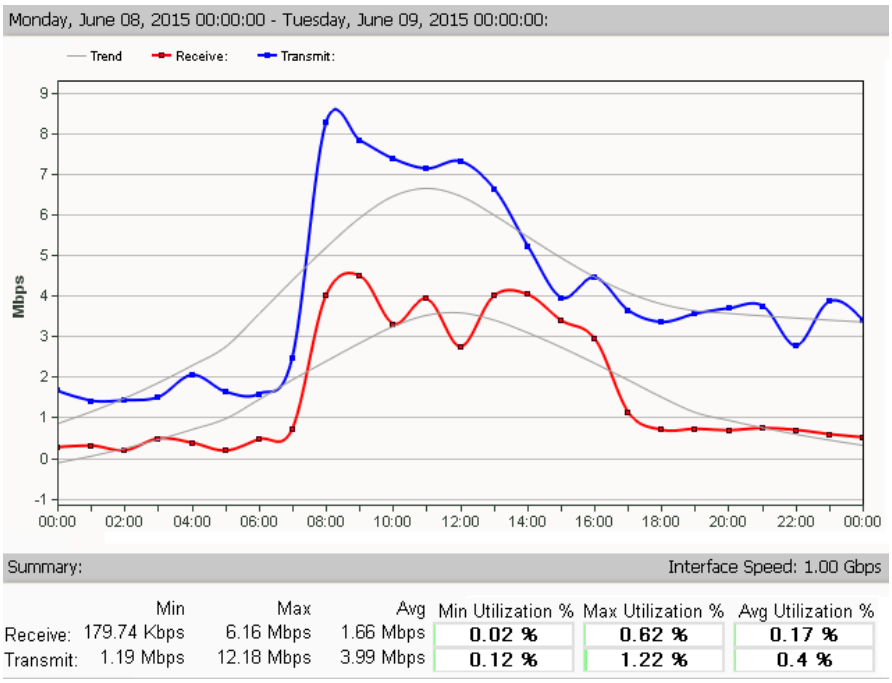
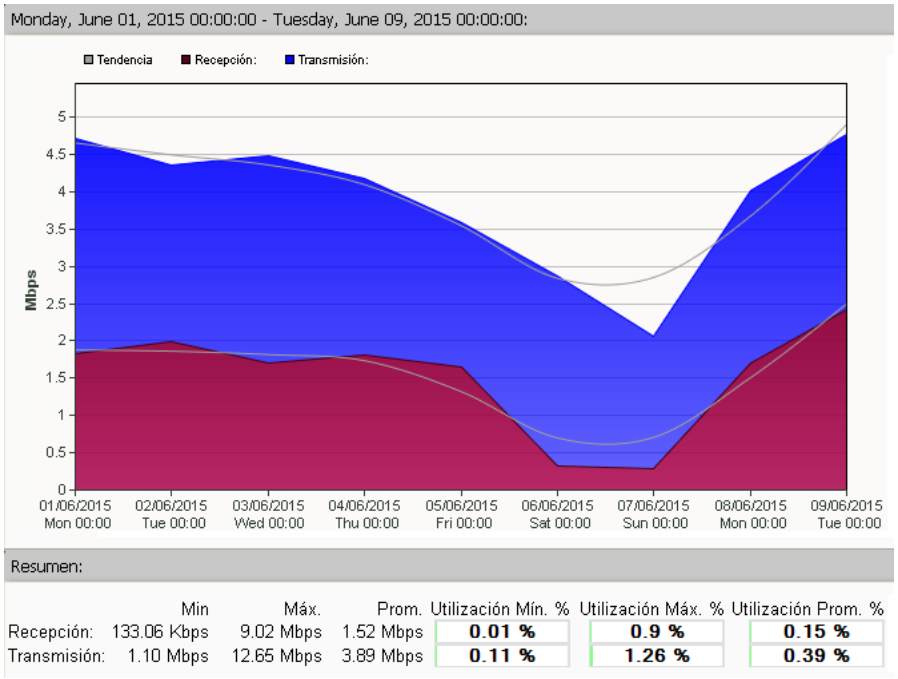


Figura 3. 72 Consumo de ancho de banda de la semana del lunes 01 al martes 09 de Junio



3.5.5.5 Enlace SWDATACENTER - SWMOTORES

Los porcentajes de mayor consumo son reportados dentro de las horas de oficina, que comprende desde las 8:00 hasta 17:00, con un consumo máximo de transmisión de 35 Mbps que y un máximo de recepción de 2.53 Mbps. Las figuras 3.73, 3.74, 3.75, 3.76 y 3.79 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 de cada día, en donde se puede evidenciar que los valores de transmisión y recepción varían durante todo el día, especialmente en el horario de oficina. Las figuras 3.77 y 3.78 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 durante el fin de semana, en donde se puede evidenciar que los valores de transmisión y recepción presentan valores bajos. La figura 3.80 muestra el monitoreo realizado durante toda la semana, en donde se puede evidenciar el consumo diario con pico de tráfico el día Lunes.

Figura 3. 73 Consumo de ancho de banda lunes 01 al martes 02 de Junio

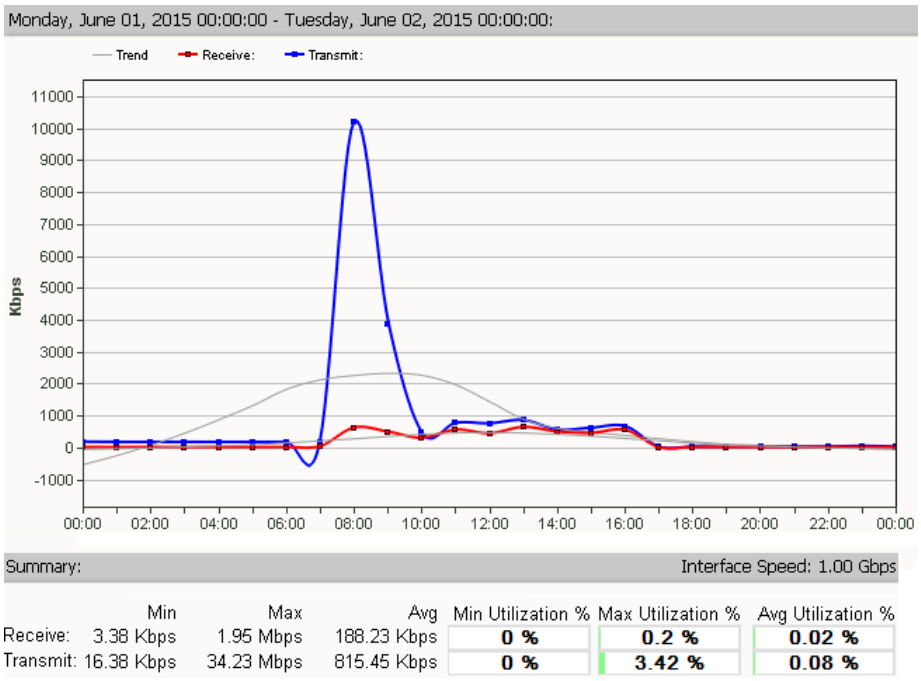


Figura 3. 74 Consumo de ancho de banda martes 02 al miércoles 03 de Junio

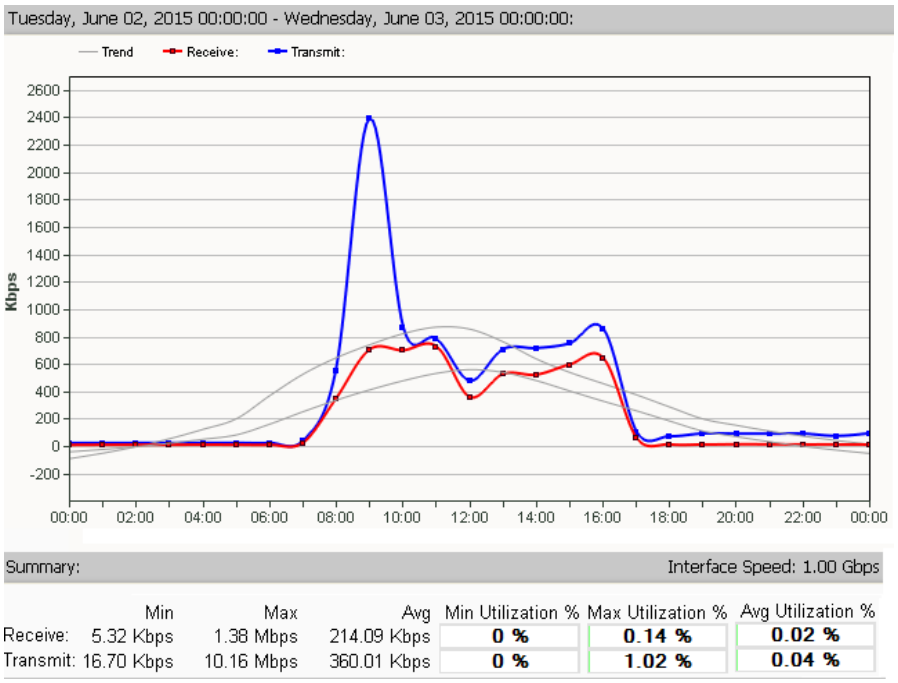


Figura 3. 75 Consumo de ancho de banda miércoles 03 al jueves 04 de Junio

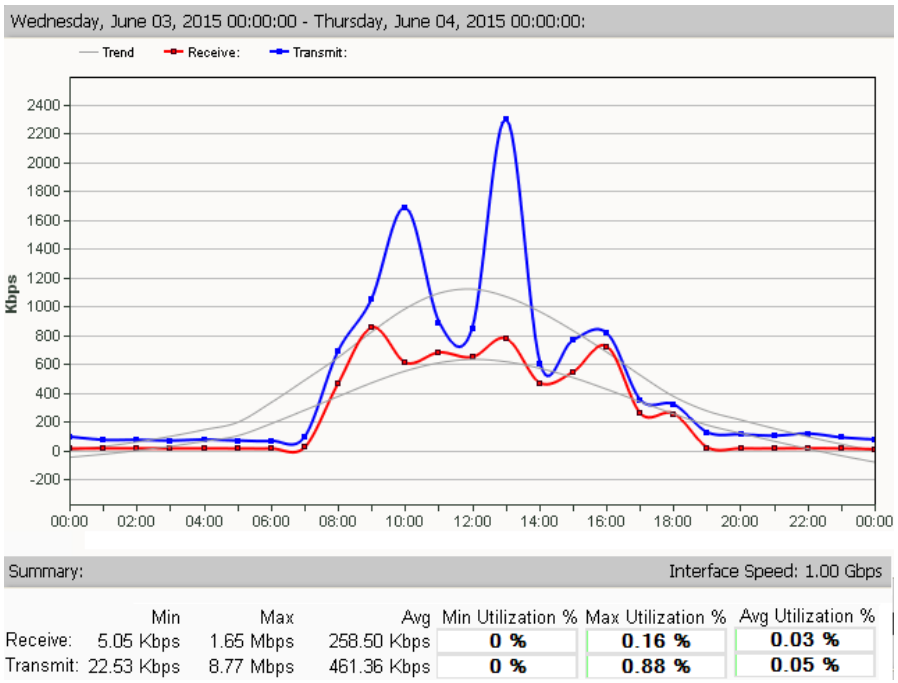
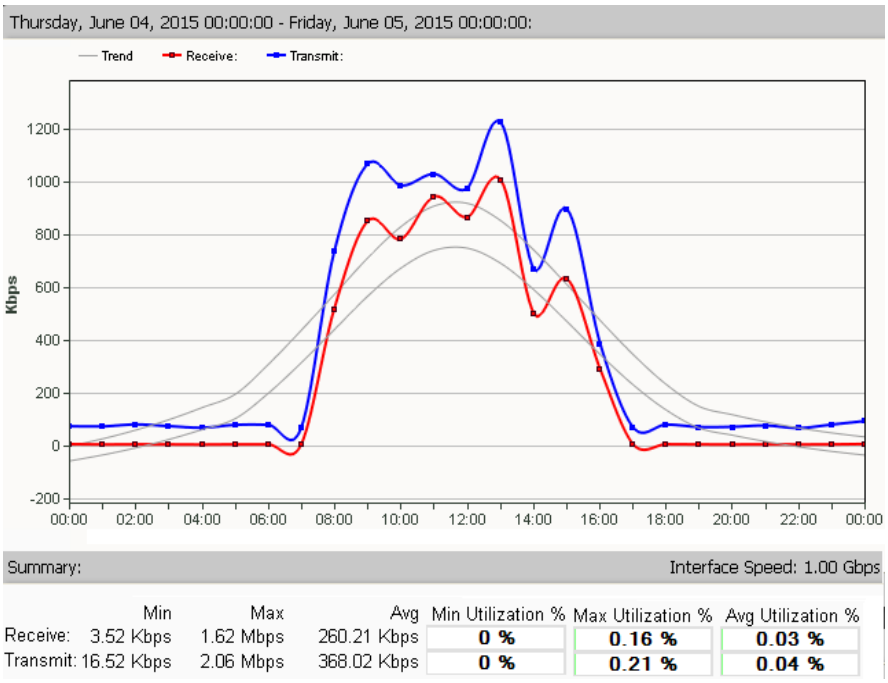
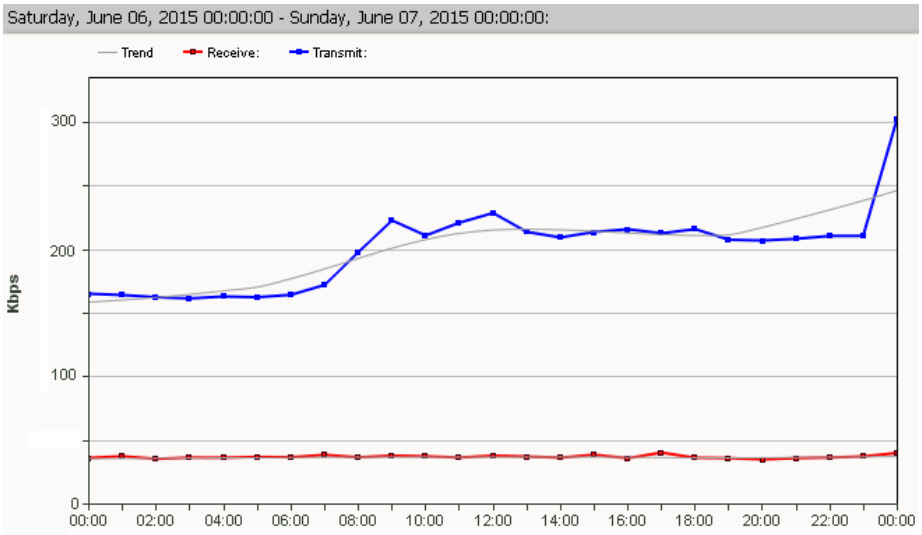


Figura 3. 76 Consumo de ancho de banda jueves 04 al viernes 05 de Junio



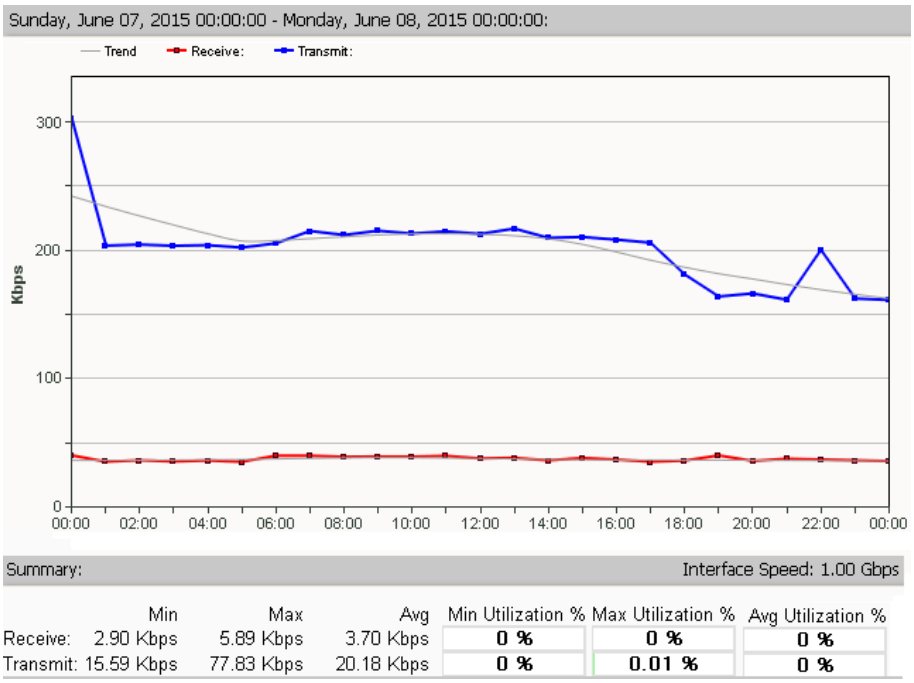
	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	3.52 Kbps	1.62 Mbps	260.21 Kbps	0 %	0.16 %	0.03 %
Transmit:	16.52 Kbps	2.06 Mbps	368.02 Kbps	0 %	0.21 %	0.04 %

Figura 3. 77 Consumo de ancho de banda sábado 06 al domingo 07 de Junio



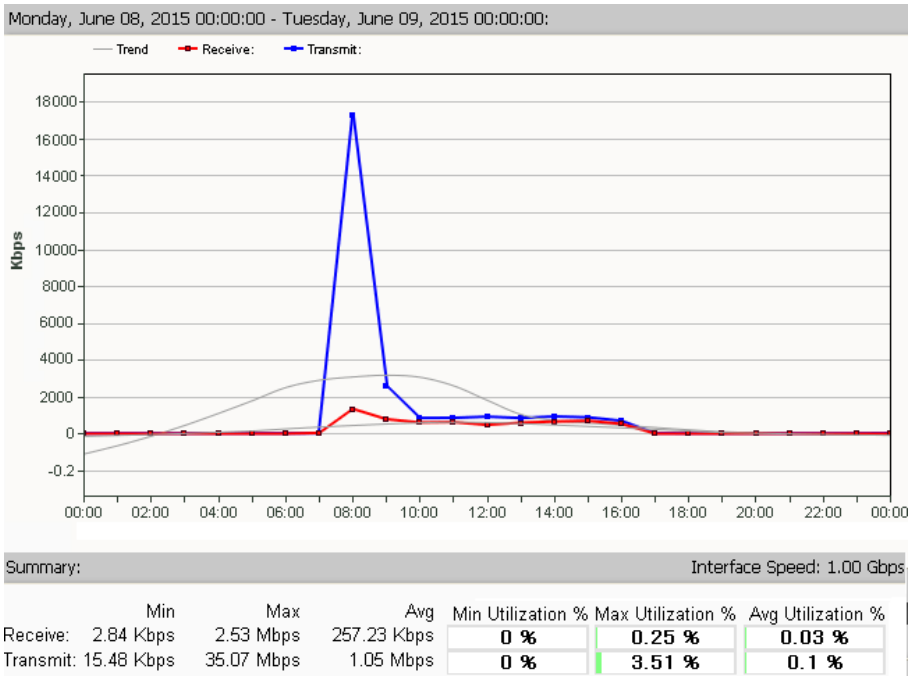
	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	2.88 Kbps	6.34 Kbps	3.67 Kbps	0 %	0 %	0 %
Transmit:	15.81 Kbps	77.83 Kbps	20.07 Kbps	0 %	0.01 %	0 %

Figura 3. 78 Consumo de ancho de banda domingo 07 al lunes 08 de Junio



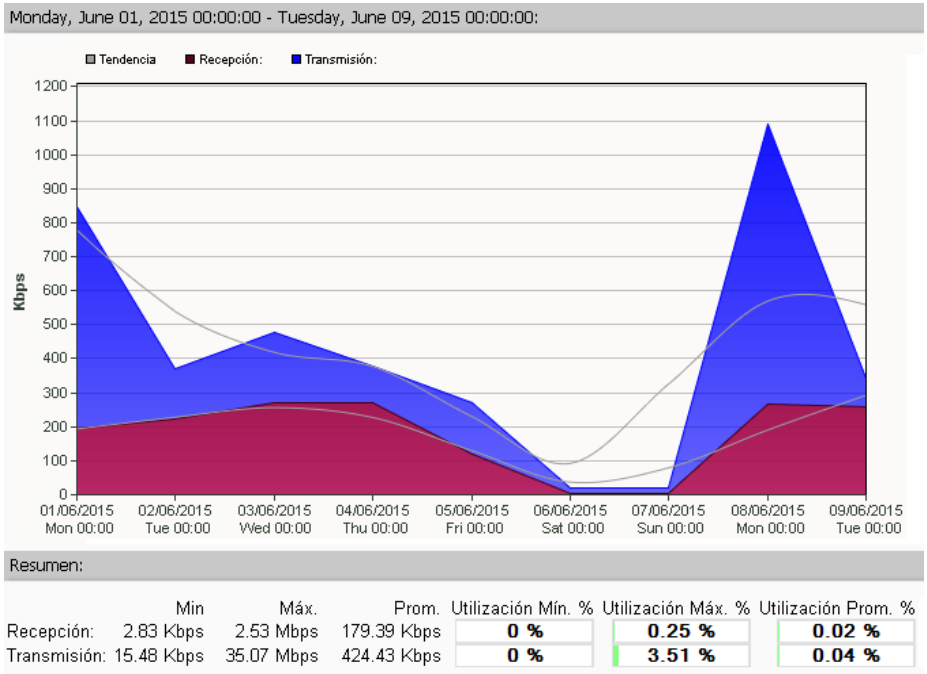
	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	2.90 Kbps	5.89 Kbps	3.70 Kbps	0 %	0 %	0 %
Transmit:	15.59 Kbps	77.83 Kbps	20.18 Kbps	0 %	0.01 %	0 %

Figura 3. 79 Consumo de ancho de banda lunes 08 al martes 09 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	2.84 Kbps	2.53 Mbps	257.23 Kbps	0 %	0.25 %	0.03 %
Transmit:	15.48 Kbps	35.07 Mbps	1.05 Mbps	0 %	3.51 %	0.1 %

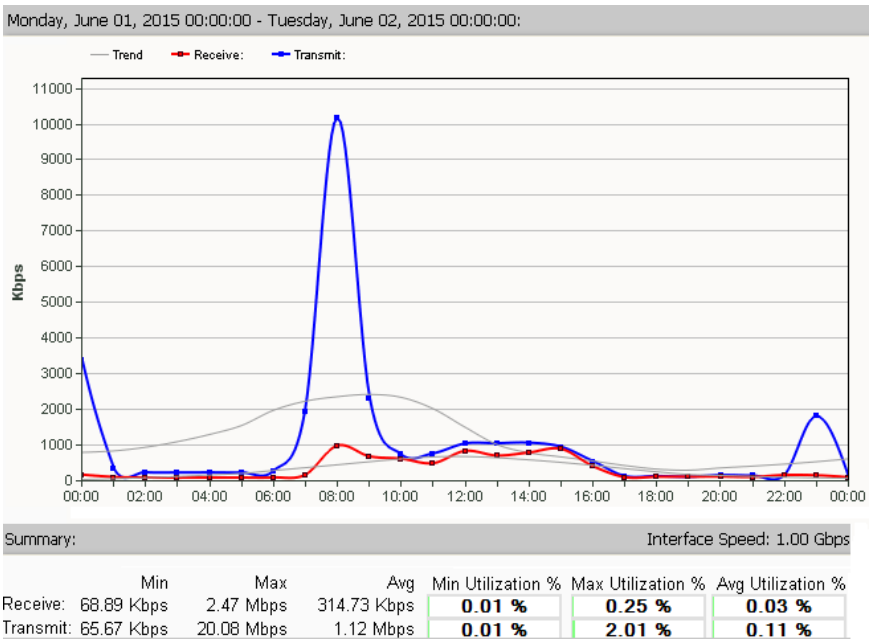
Figura 3. 80 Consumo de ancho de banda de la semana del lunes 01 al martes 09 de Junio



3.5.5.6 Enlace SWDATACENTER - SWLABORATORIO

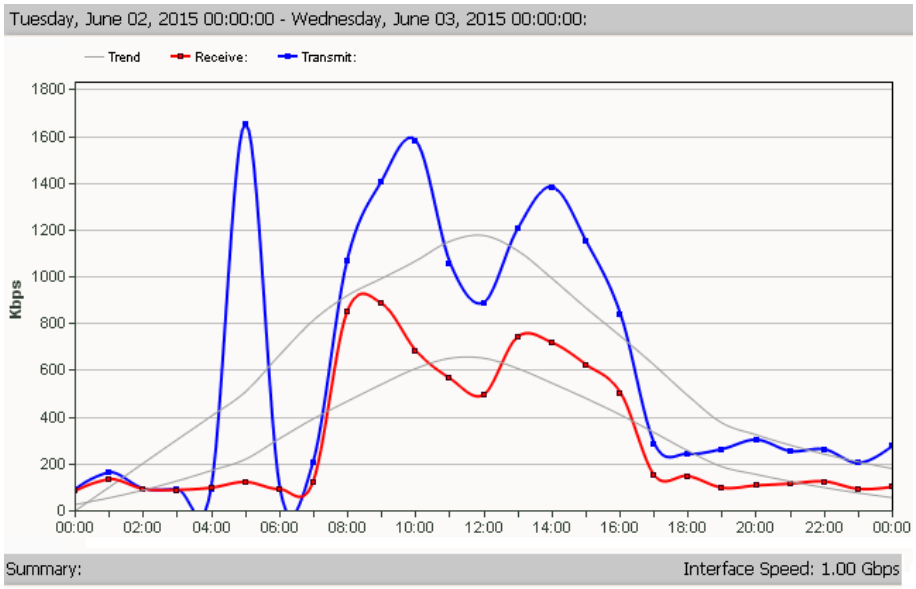
Los porcentajes de mayor consumo son reportados dentro de las horas de oficina, que comprende desde las 8:00 hasta 17:00, con un consumo máximo de transmisión de 20 Mbps un máximo de recepción de 10 Mbps. Las figuras 3.81, 3.82, 3.83, 3.84 y 3.87 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 de cada día, en donde se puede evidenciar que los valores de transmisión y recepción varían durante todo el día, especialmente en el horario de oficina. Las figuras 3.85 y 3.86 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 durante el fin de semana, en donde se puede evidenciar que los valores de transmisión y recepción presentan valores bajos. La figura 3.88 muestra el monitoreo realizado durante toda la semana, en donde se puede evidenciar el consumo diario y el pico de tráfico el día Lunes.

Figura 3. 81 Consumo de ancho de banda lunes 01 al martes 02 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	68.89 Kbps	2.47 Mbps	314.73 Kbps	0.01 %	0.25 %	0.03 %
Transmit:	65.67 Kbps	20.08 Mbps	1.12 Mbps	0.01 %	2.01 %	0.11 %

Figura 3. 82 Consumo de ancho de banda martes 02 al miércoles 03 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	75.88 Kbps	1.28 Mbps	311.18 Kbps	0.01 %	0.13 %	0.03 %
Transmit:	70.62 Kbps	9.49 Mbps	603.04 Kbps	0.01 %	0.95 %	0.06 %

Figura 3. 83 Consumo de ancho de banda miércoles 03 al jueves 04 de Junio

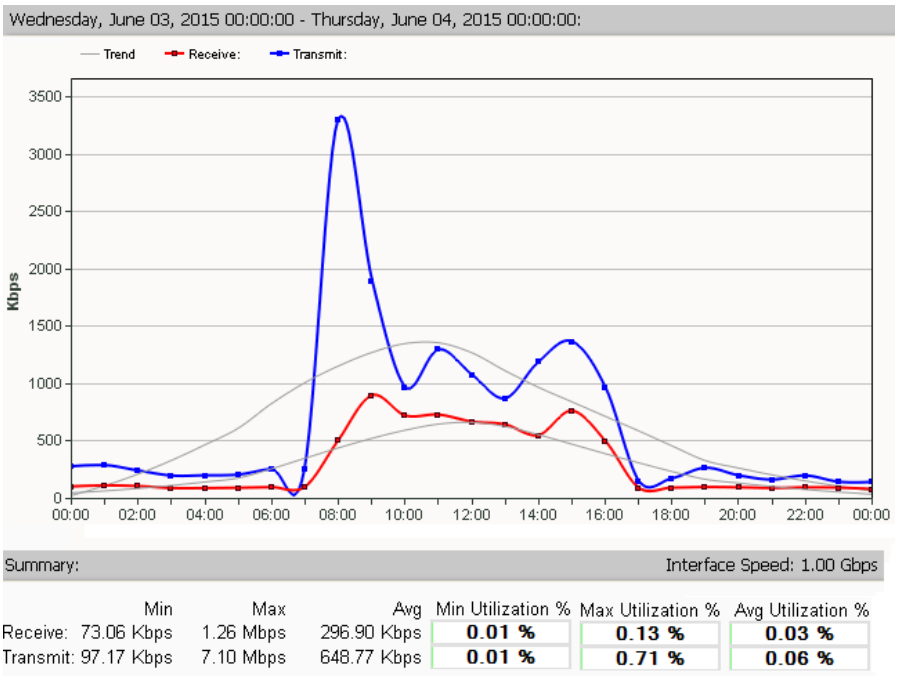


Figura 3. 84 Consumo de ancho de banda jueves 04 al viernes 05 de Junio

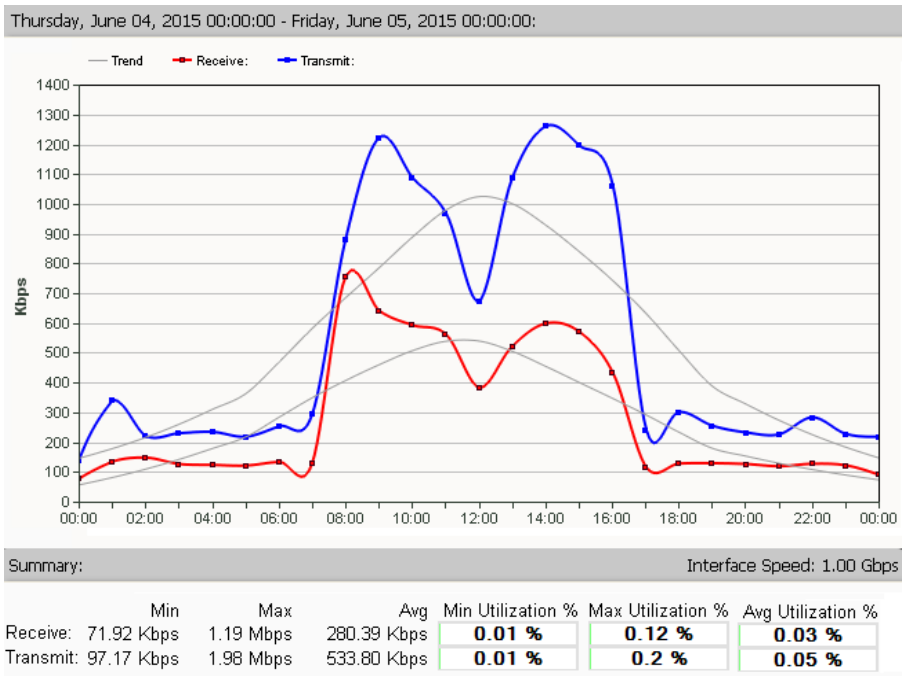
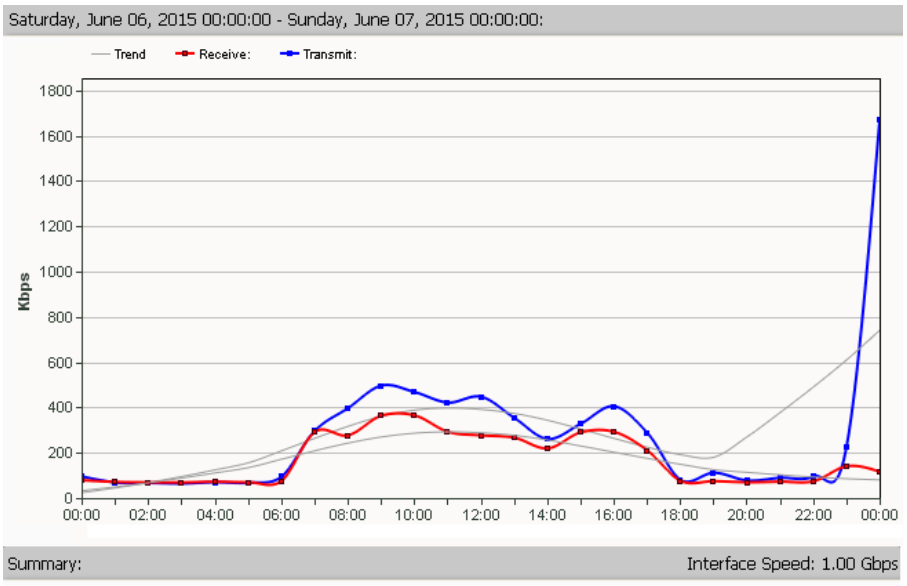
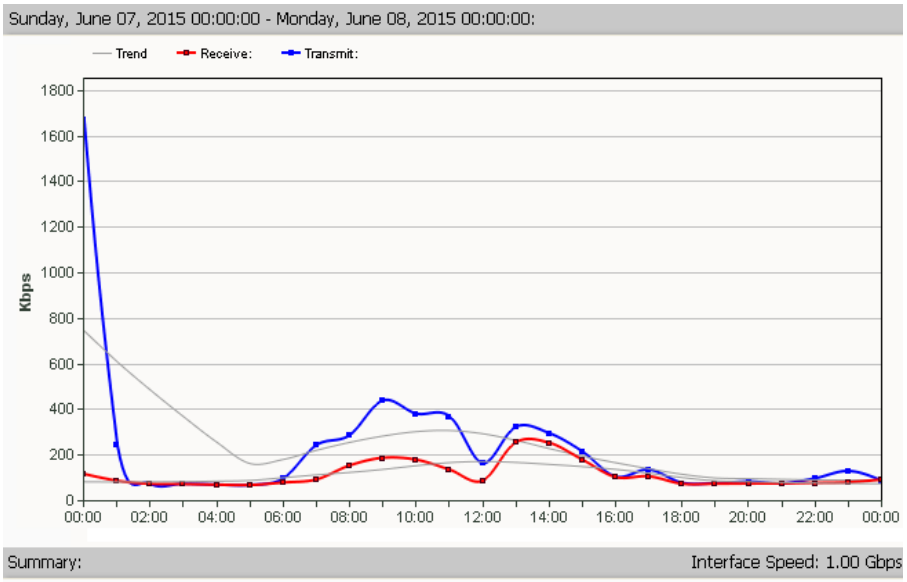


Figura 3. 85 Consumo de ancho de banda sábado 06 al domingo 07 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	65.98 Kbps	986.95 Kbps	170.15 Kbps	0.01 %	0.1 %	0.02 %
Transmit:	60.25 Kbps	9.54 Mbps	281.08 Kbps	0.01 %	0.95 %	0.03 %

Figura 3. 86 Consumo de ancho de banda domingo 07 al lunes 08 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	63.84 Kbps	541.33 Kbps	112.12 Kbps	0.01 %	0.05 %	0.01 %
Transmit:	59.74 Kbps	9.54 Mbps	233.54 Kbps	0.01 %	0.95 %	0.02 %

Figura 3. 87 Consumo de ancho de banda lunes 08 al martes 09 de Junio

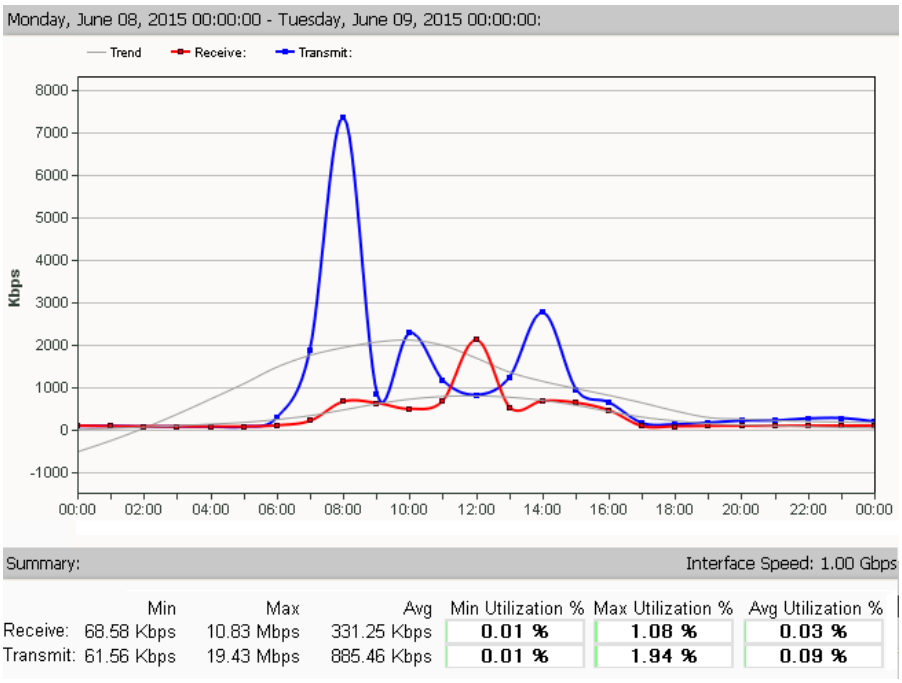
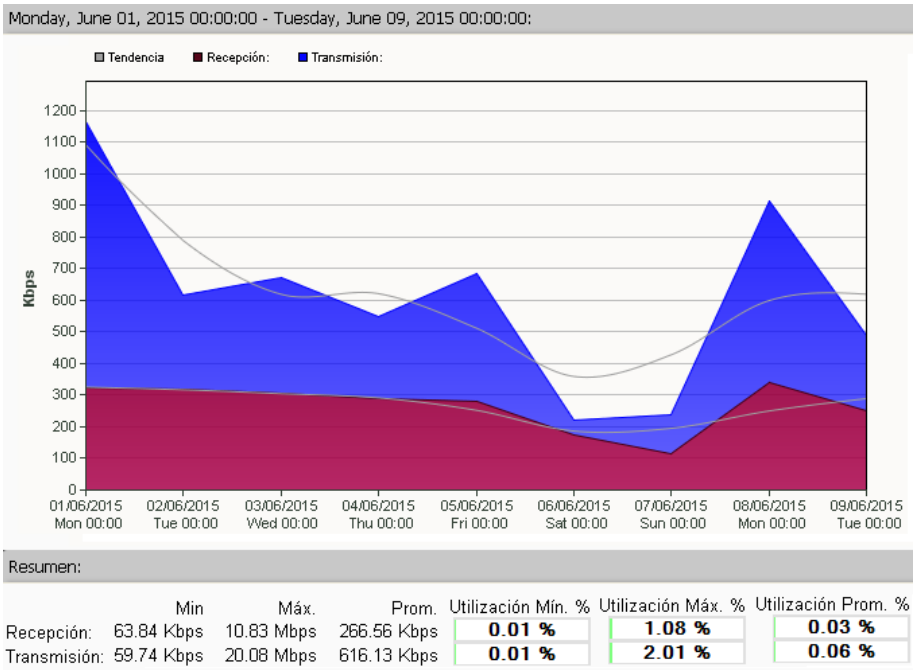


Figura 3. 88 Consumo de ancho de banda de la semana del lunes 01 al martes 09 de Junio



3.5.5.7 Enlace SWDATACENTER - SWQUITO

Los porcentajes de mayor consumo son reportados dentro de las horas de oficina, que comprende desde las 8:00 hasta 17:00, con un consumo máximo de transmisión de 45.6 Mbps y un máximo de recepción de 44.5 Mbps. Las figuras 3.89, 3.90, 3.91, 3.92 y 3.95 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 de cada día, en donde se puede evidenciar que los valores de transmisión y recepción varían durante todo el día, especialmente en el horario de oficina. Adicionalmente de observa a las 4:00 un valor alto de recepción debido a las actividades de respaldo de las Oficinas de Quito. Las figuras 3.93 y 3.94 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 durante el fin de semana, en donde se puede evidenciar que los valores de transmisión y recepción presentan valores bajos. La figura 3.96 muestra el monitoreo realizado durante toda la semana, en donde se puede evidenciar el consumo diario y el pico de tráfico el día Lunes.

Figura 3. 89 Consumo de ancho de banda lunes 01 al martes 02 de Junio

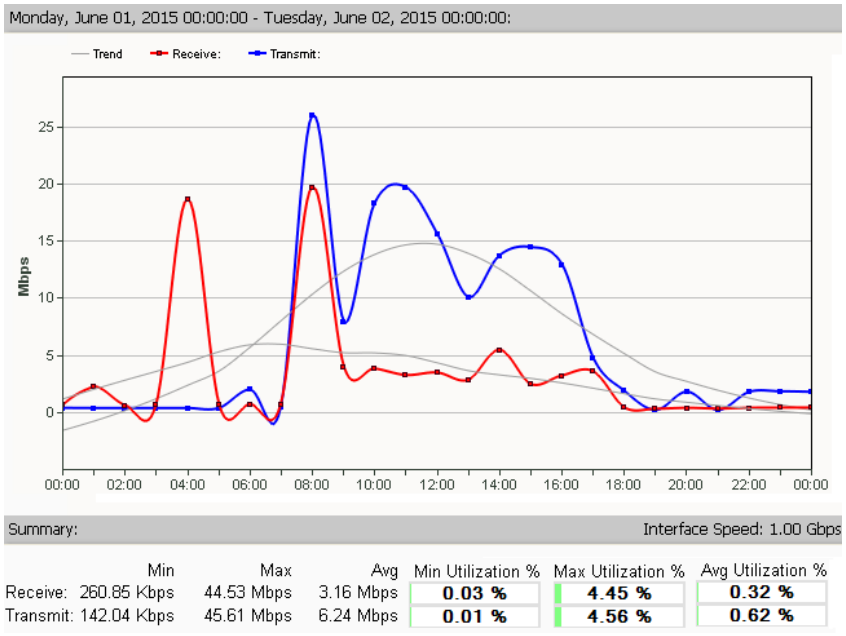
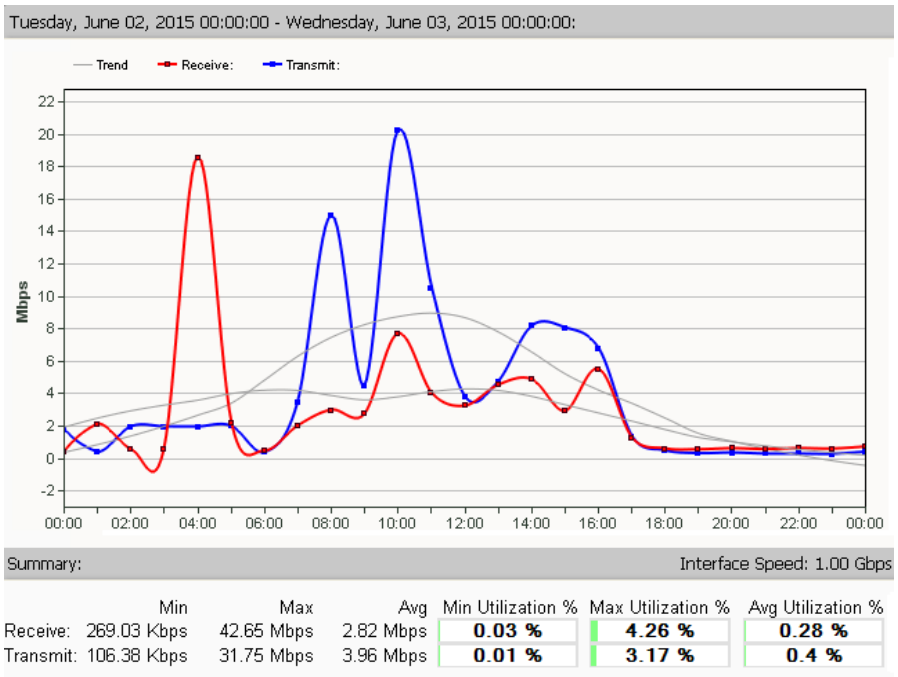
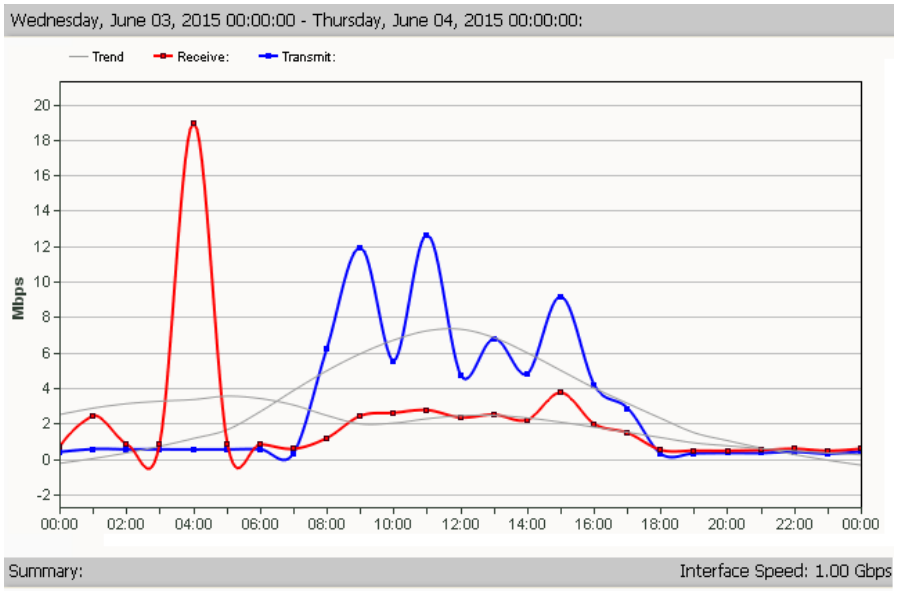


Figura 3. 90 Consumo de ancho de banda martes 02 al miércoles 03 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	269.03 Kbps	42.65 Mbps	2.82 Mbps	0.03 %	4.26 %	0.28 %
Transmit:	106.38 Kbps	31.75 Mbps	3.96 Mbps	0.01 %	3.17 %	0.4 %

Figura 3. 91 Consumo de ancho de banda miércoles 03 al jueves 04 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	394.77 Kbps	41.54 Mbps	2.10 Mbps	0.04 %	4.15 %	0.21 %
Transmit:	192.08 Kbps	23.80 Mbps	3.00 Mbps	0.02 %	2.38 %	0.3 %

Figura 3. 92 Consumo de ancho de banda jueves 04 al viernes 05 de Junio

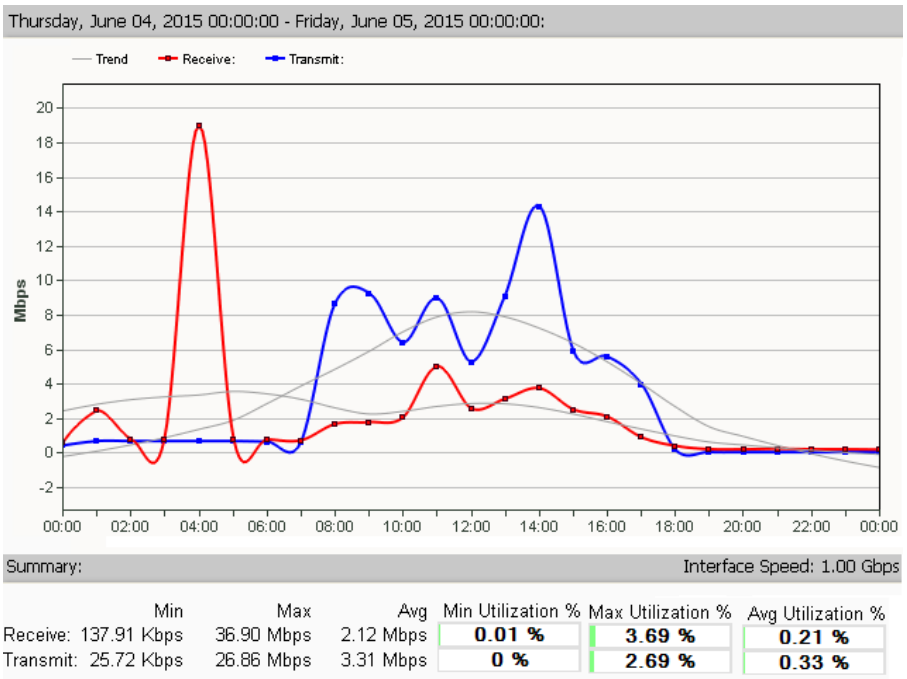


Figura 3. 93 Consumo de ancho de banda sábado 06 al domingo 07 de Junio

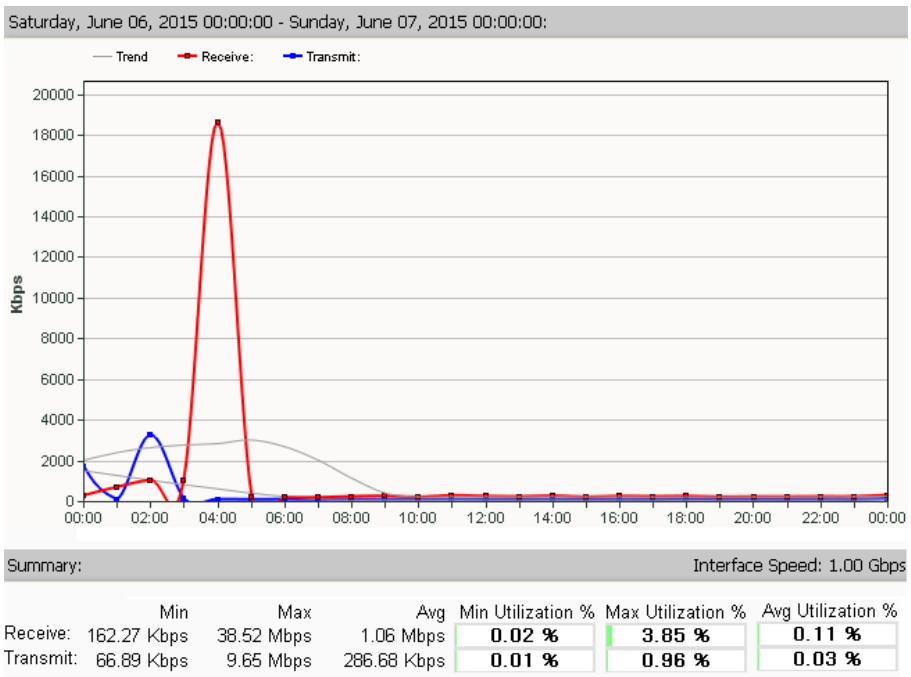


Figura 3. 94 Consumo de ancho de banda domingo 07 al lunes 08 de Junio

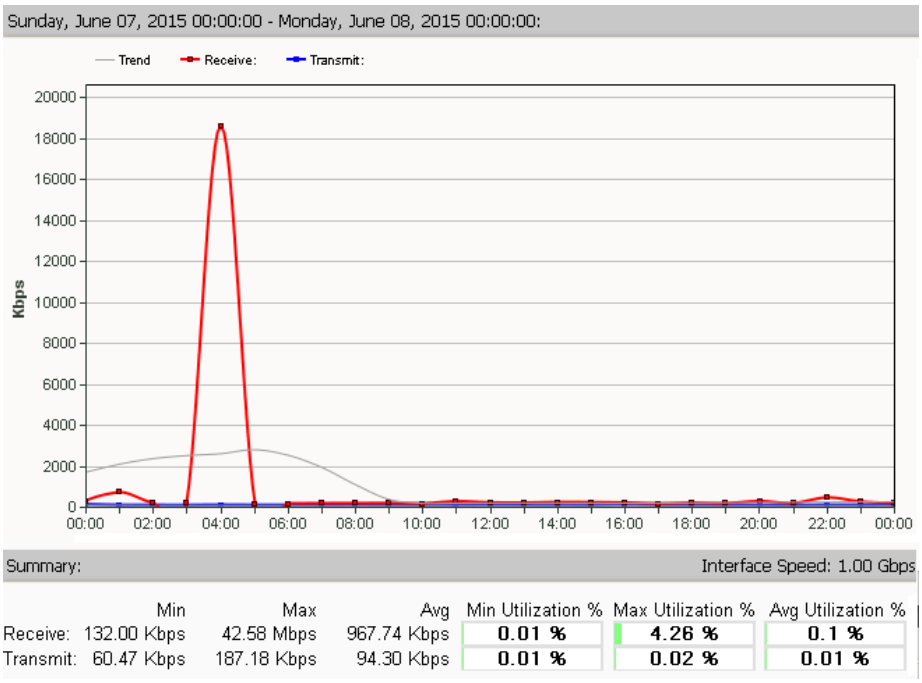


Figura 3. 95 Consumo de ancho de banda lunes 08 al martes 09 de Junio

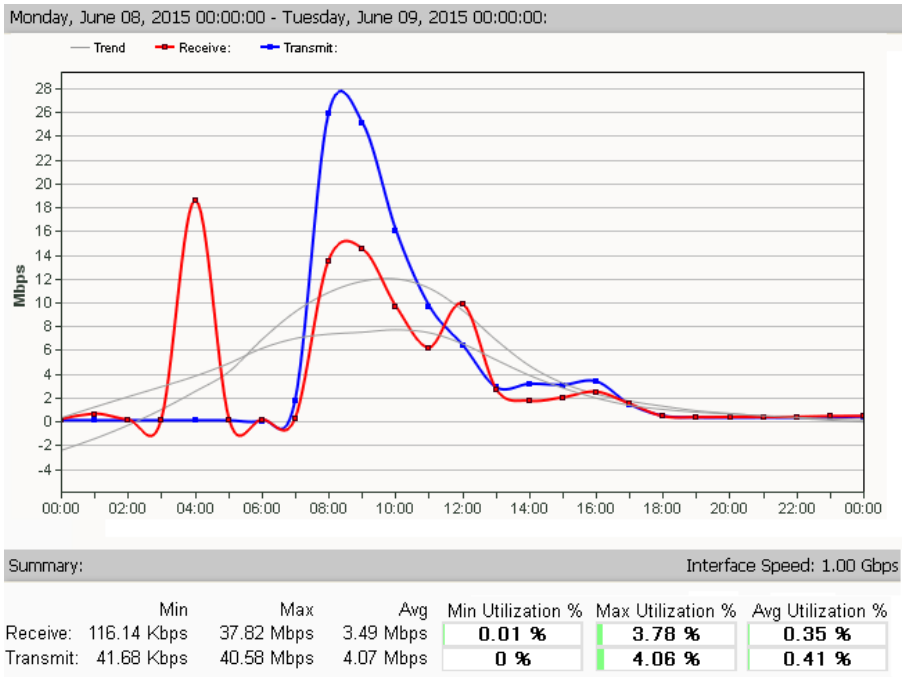
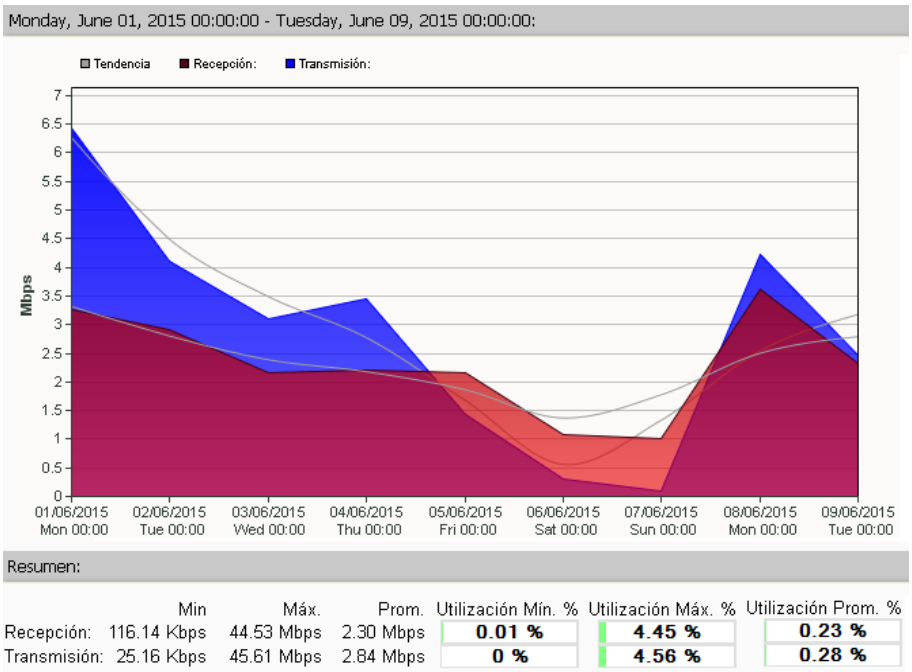


Figura 3. 96 Consumo de ancho de banda de la semana del lunes 01 al martes 09 de Junio



3.5.5.8 Enlace SWDATACENTER - SWARCHIVO

Los porcentajes de mayor consumo son reportados dentro de las horas de oficina, que comprende desde las 8:00 hasta 17:00, con un consumo máximo de transmisión de 22.8 Mbps y un máximo de recepción de 10.9 Mbps. Las figuras 3.97, 3.98, 3.99, 3.100 y 3.103 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 de cada día, en donde se puede evidenciar que los valores de transmisión y recepción varían durante todo el día y especialmente en horarios de oficina. Las figuras 3.101 y 3.102 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 durante el fin de semana, en donde se puede evidenciar que los valores de transmisión y recepción presentan valores bajos. La figura 3.103 muestra el monitoreo realizado durante toda la semana, en donde se puede evidenciar el consumo diario y el pico de tráfico del día Lunes.

Figura 3. 97 Consumo de ancho de banda lunes 01 al martes 02 de Junio

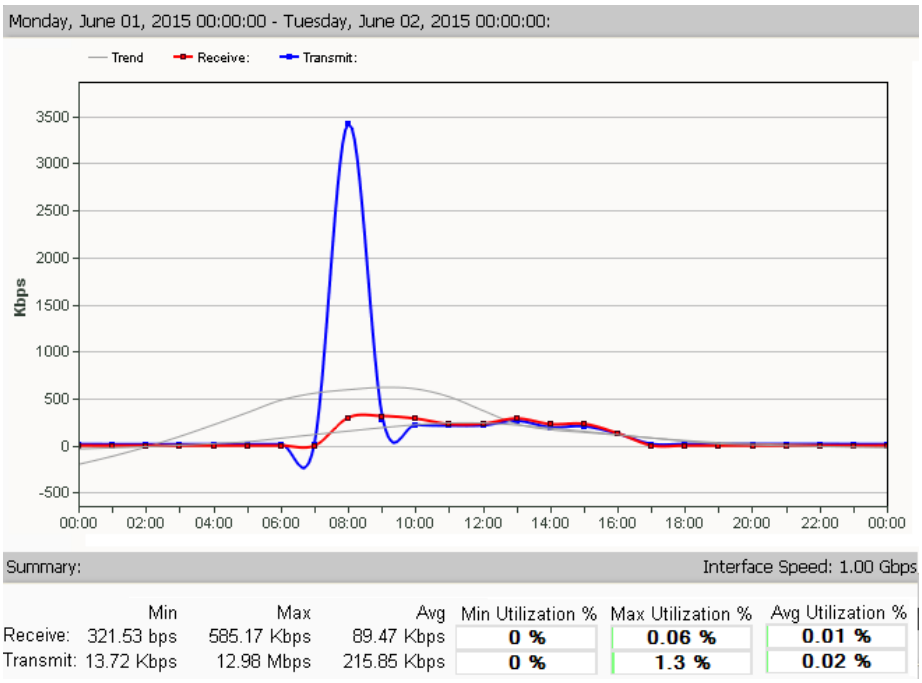


Figura 3. 98 Consumo de ancho de banda martes 02 al miércoles 03 de Junio

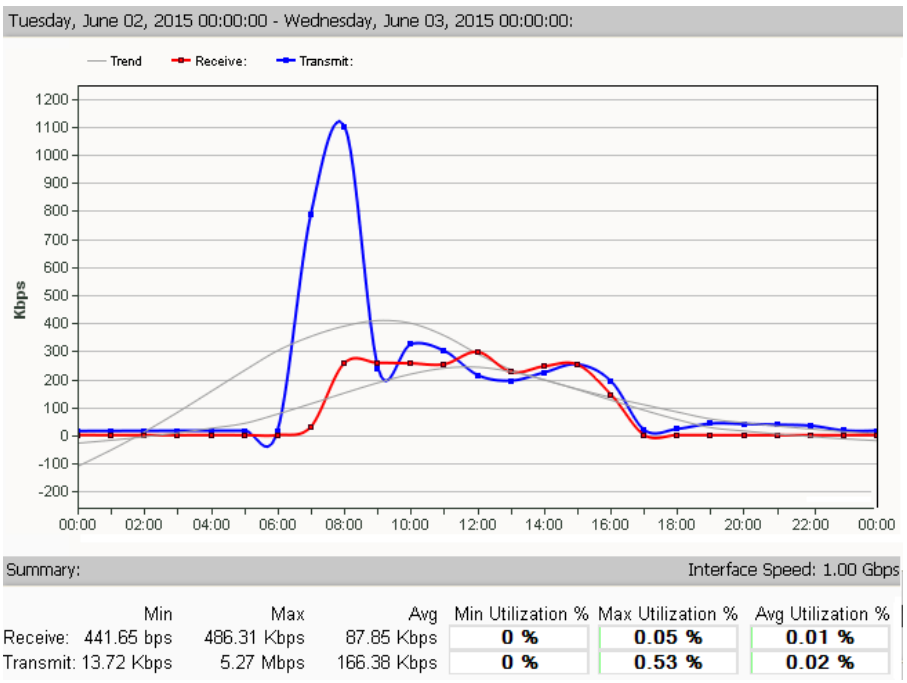


Figura 3. 99 Consumo de ancho de banda miércoles 03 al jueves 04 de Junio

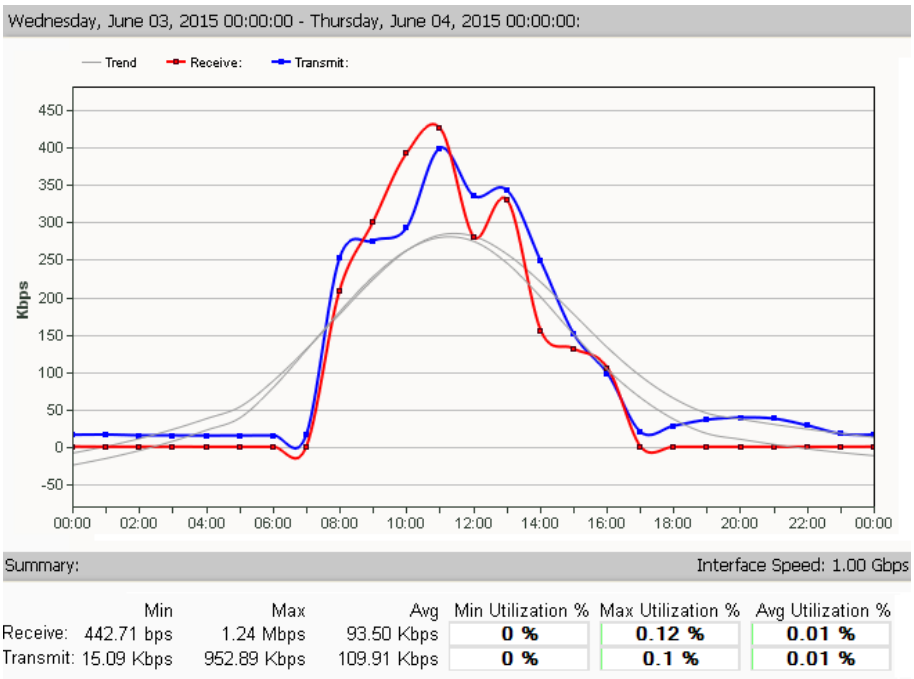


Figura 3. 100 Consumo de ancho de banda jueves 04 al viernes 05 de Junio

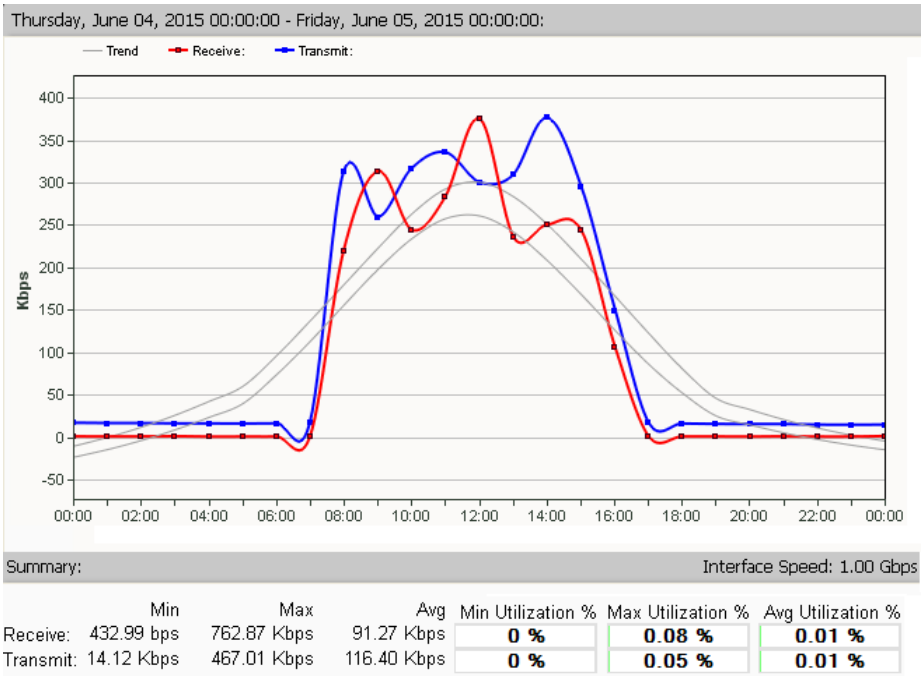
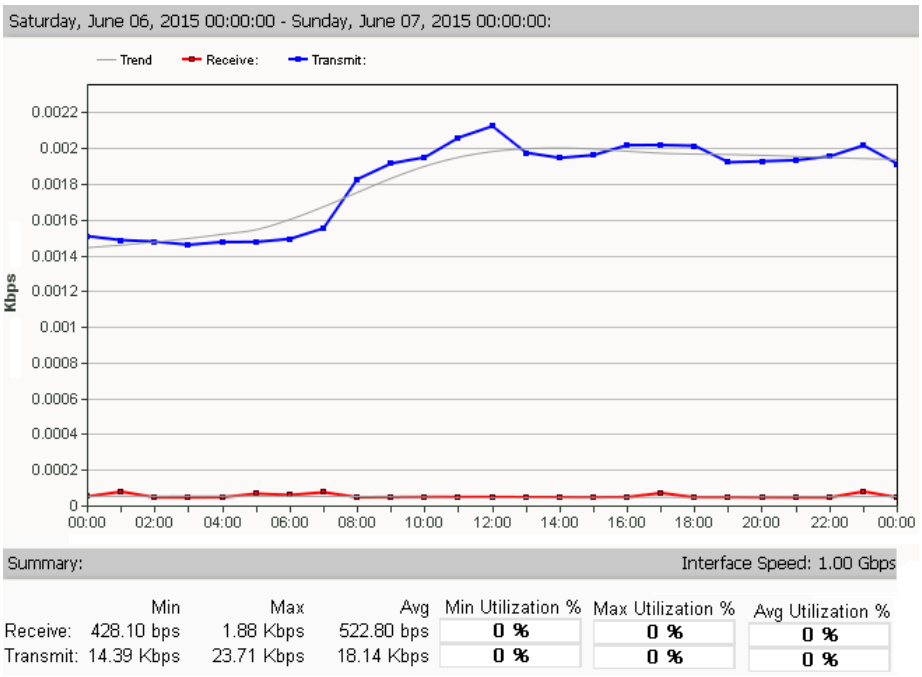
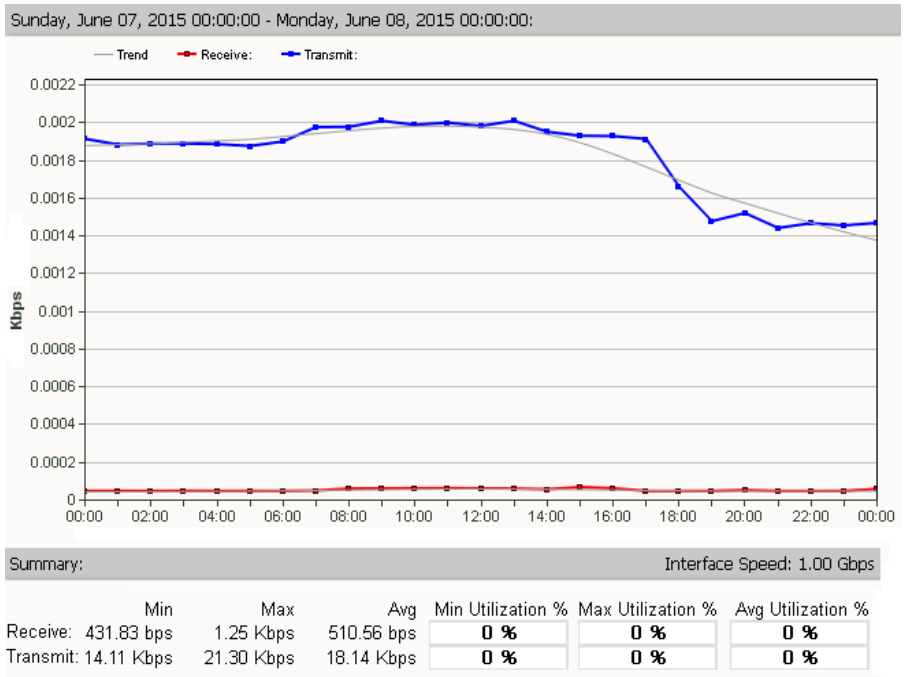


Figura 3. 101 Consumo de ancho de banda sábado 06 al domingo 07 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	428.10 bps	1.88 Kbps	522.80 bps	0 %	0 %	0 %
Transmit:	14.39 Kbps	23.71 Kbps	18.14 Kbps	0 %	0 %	0 %

Figura 3. 102 Consumo de ancho de banda domingo 07 al lunes 08 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	431.83 bps	1.25 Kbps	510.56 bps	0 %	0 %	0 %
Transmit:	14.11 Kbps	21.30 Kbps	18.14 Kbps	0 %	0 %	0 %

Figura 3. 103 Consumo de ancho de banda lunes 08 al martes 09 de Junio

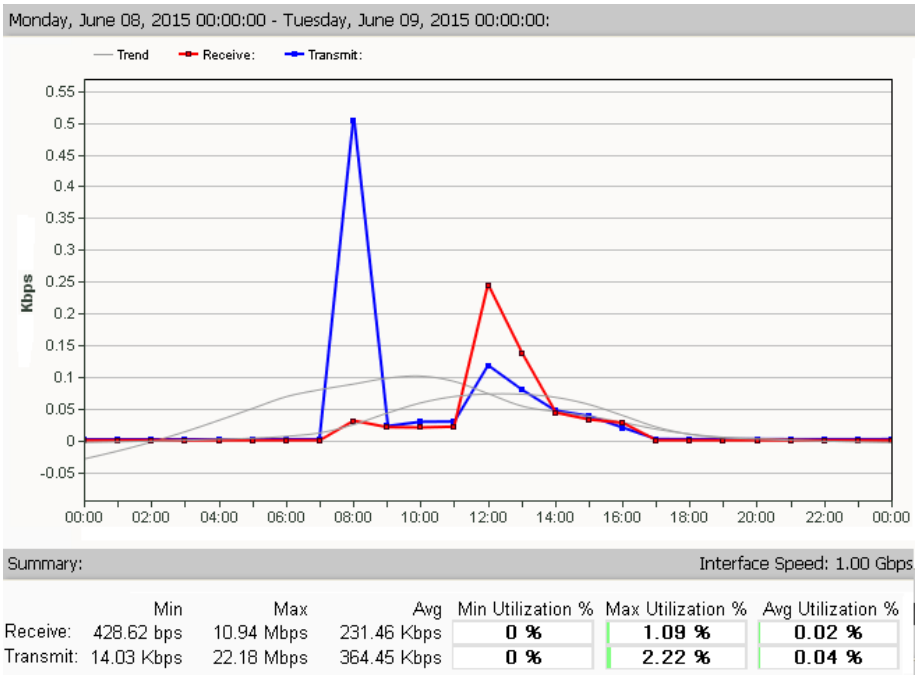
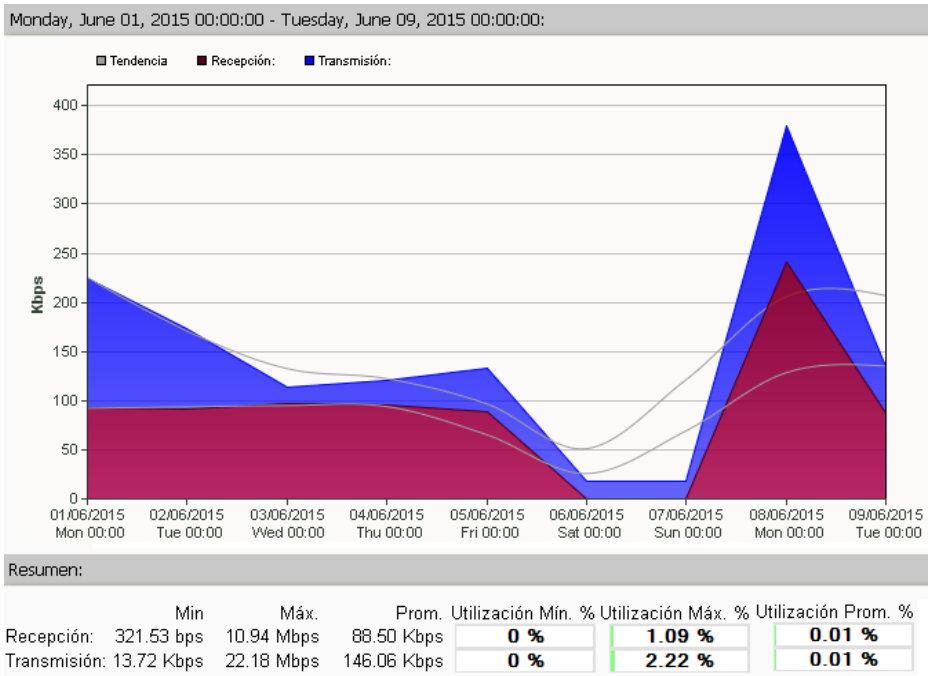


Figura 3. 104 Consumo de ancho de banda de la semana del lunes 01 al martes 09 de Junio



3.5.5.9 Enlace ROUTER GUANGOPOLO - ROUTER QUITO

Los porcentajes de mayor consumo son reportados dentro de las horas de oficina, que comprende desde las 8:00 hasta 17:00, con un consumo máximo de transmisión de 12.2 Mbps y un máximo de recepción de 9.3 Mbps. Las figuras 3.105, 3.106, 3.107, 3.108 y 3.111 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 de cada día, en donde se puede evidenciar que los valores de transmisión y recepción varían durante todo el día y especialmente en horarios de oficina. Las figuras 3.109 y 3.110 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 durante el fin de semana, en donde se puede evidenciar que los valores de transmisión y recepción presentan valores bajos. La figura 3.112 muestra el monitoreo realizado durante toda la semana, en donde se puede evidenciar el consumo diario.

Figura 3. 105 Consumo de ancho de banda lunes 01 al martes 02 de Junio

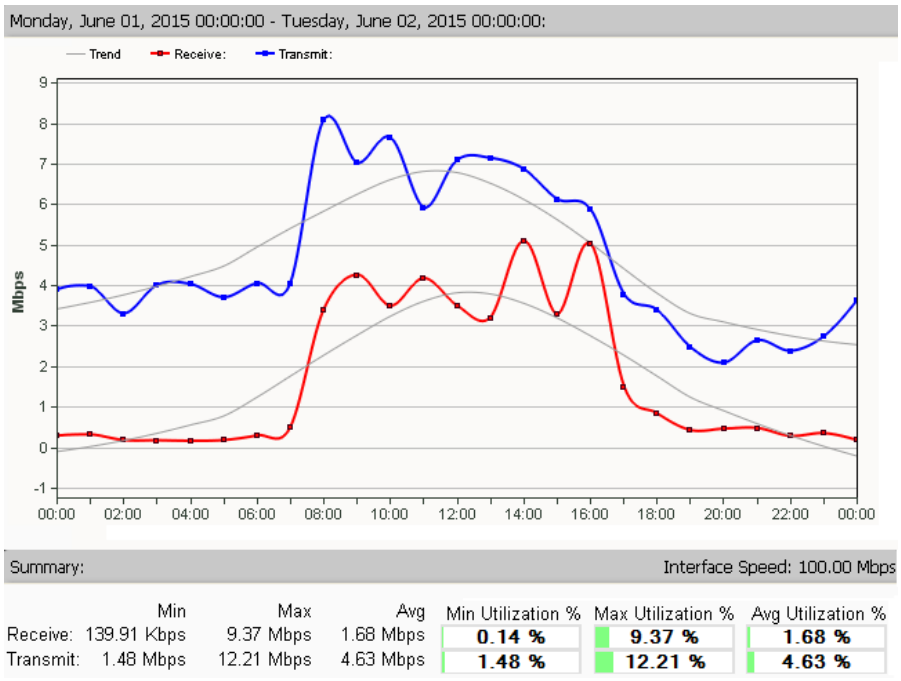


Figura 3. 106 Consumo de ancho de banda martes 02 al miércoles 03 de Junio

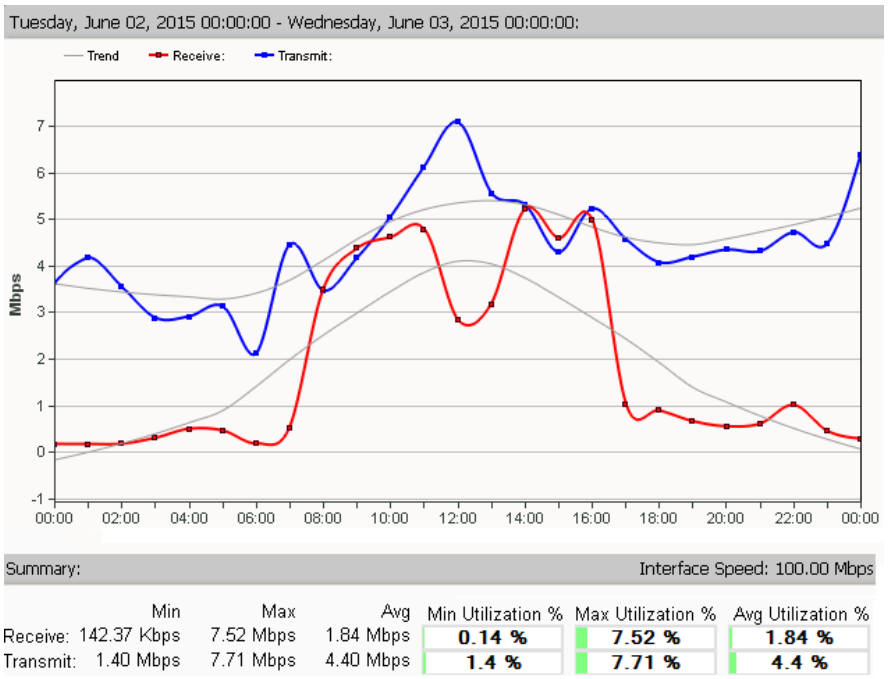


Figura 3. 107 Consumo de ancho de banda miércoles 03 al jueves 04 de Junio

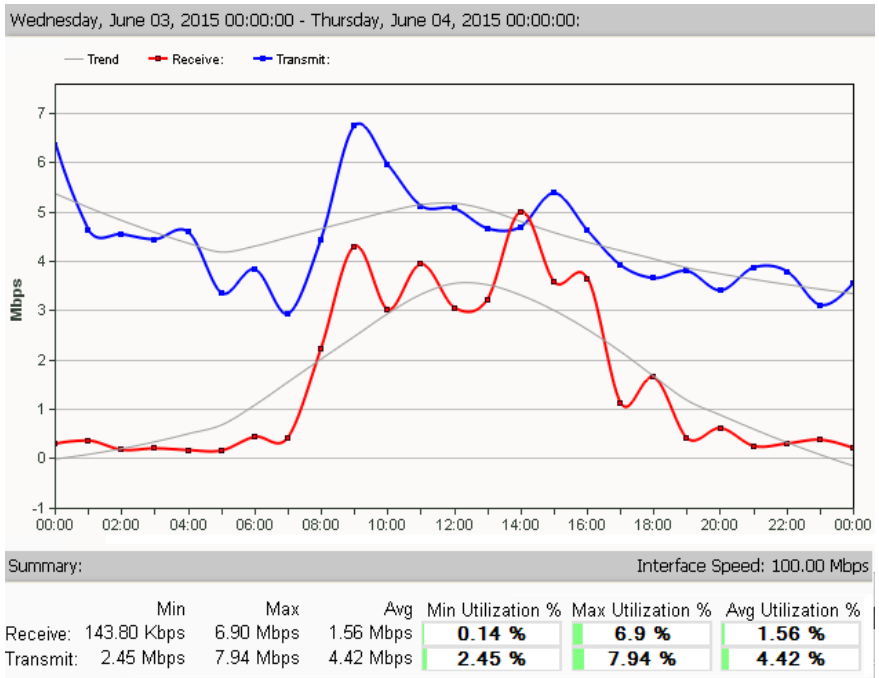
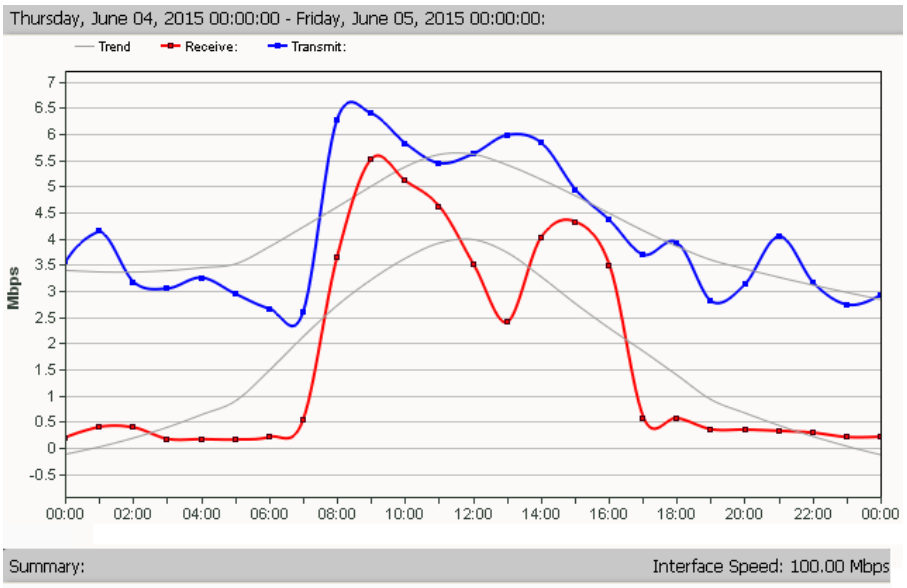


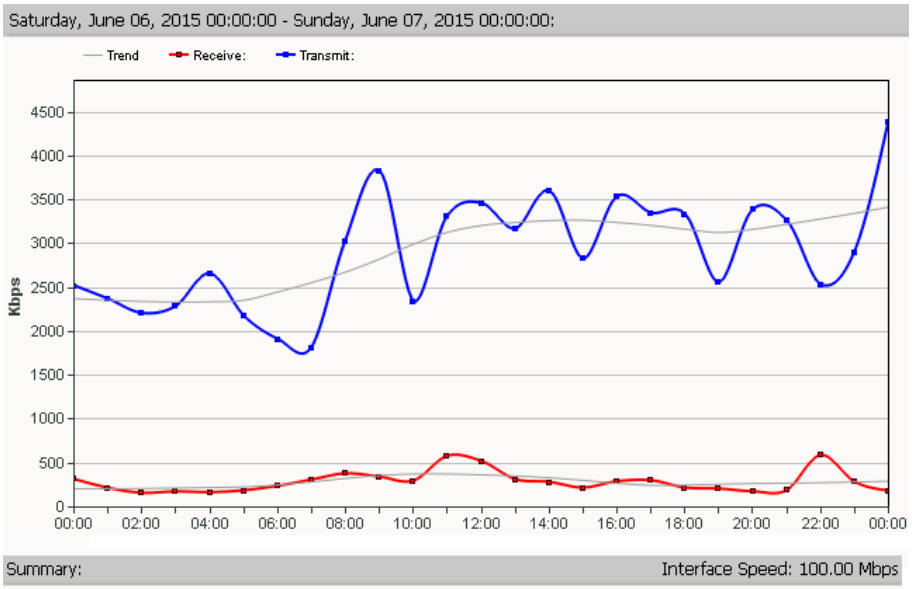
Figura 3. 108 Consumo de ancho de banda jueves 04 al viernes 05 de Junio



Summary: Interface Speed: 100.00 Mbps

	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	151.88 Kbps	6.14 Mbps	1.67 Mbps	0.15 %	6.14 %	1.67 %
Transmit:	2.25 Mbps	8.65 Mbps	4.10 Mbps	2.25 %	8.65 %	4.1 %

Figura 3. 109 Consumo de ancho de banda sábado 06 al domingo 07 de Junio



Summary: Interface Speed: 100.00 Mbps

	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	148.40 Kbps	1.19 Mbps	282.25 Kbps	0.15 %	1.19 %	0.28 %
Transmit:	1.74 Mbps	5.17 Mbps	2.91 Mbps	1.74 %	5.17 %	2.91 %

Figura 3. 110 Consumo de ancho de banda domingo 07 al lunes 08 de Junio

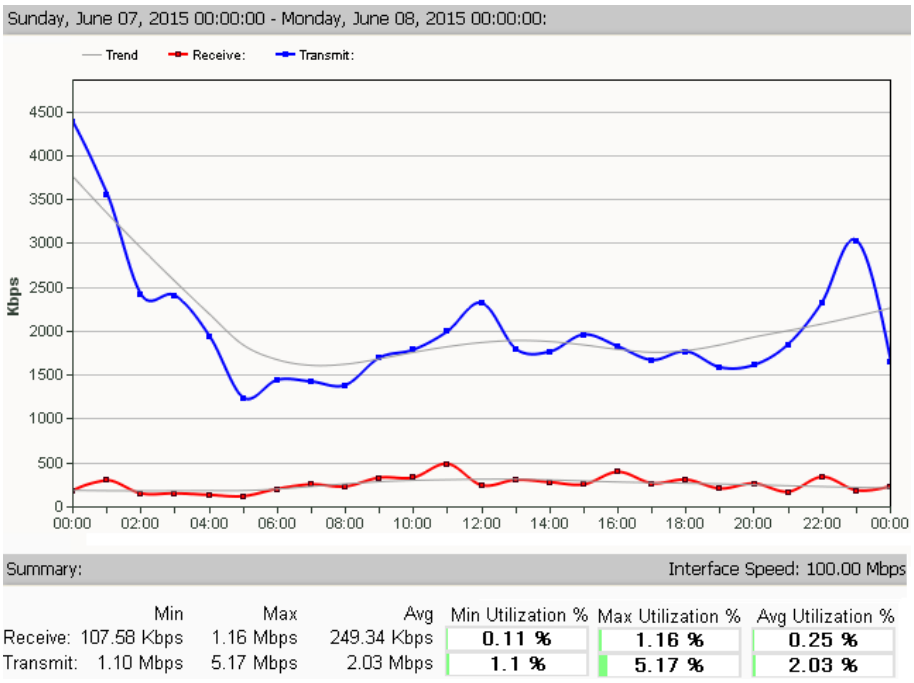


Figura 3. 111 Consumo de ancho de banda lunes 08 al martes 09 de Junio

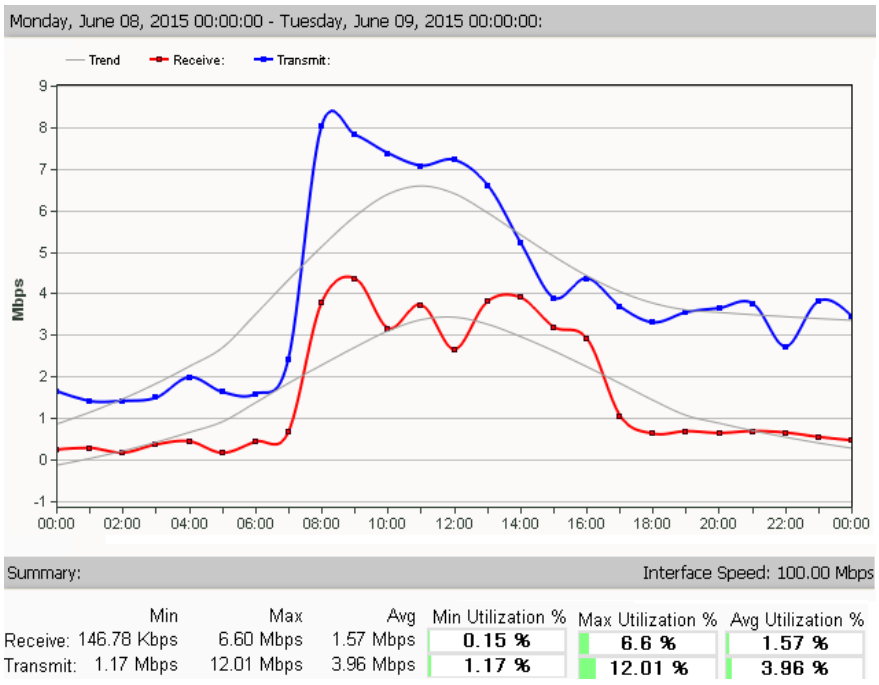
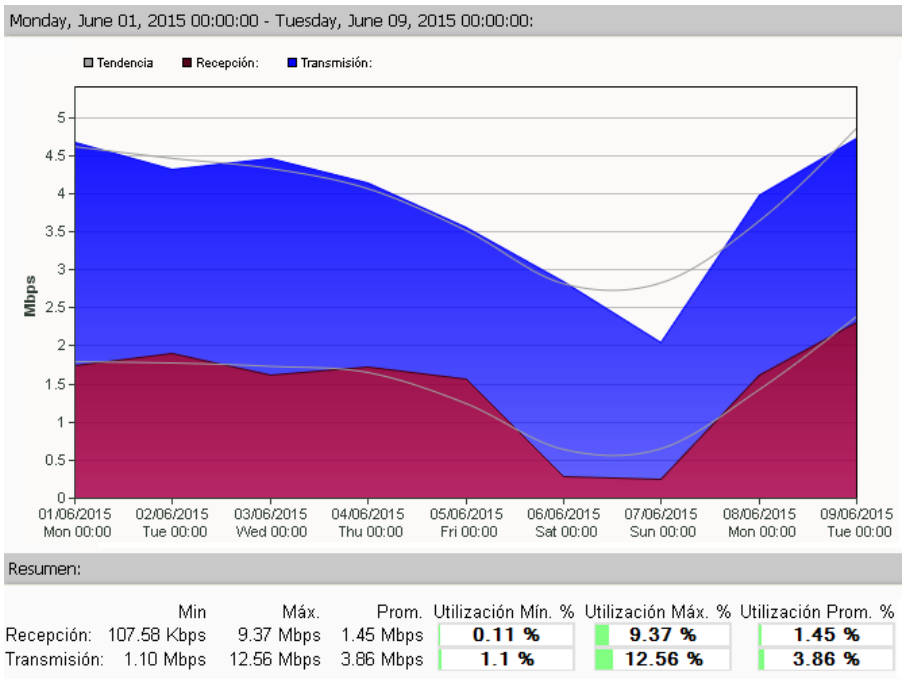


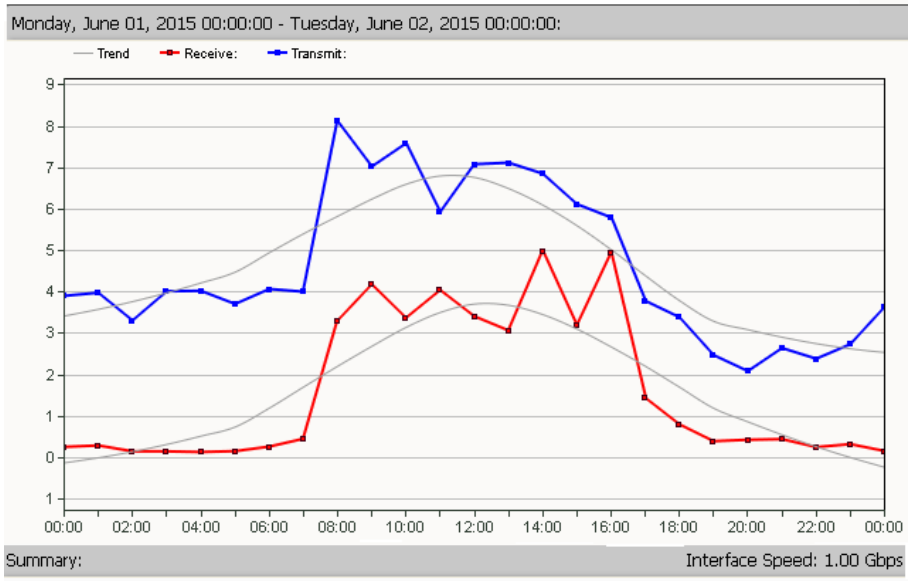
Figura 3. 112 Consumo de ancho de banda de la semana del lunes 01 al martes 09 de Junio



3.5.5.10 Enlace ROUTER QUITO - FIREWALL

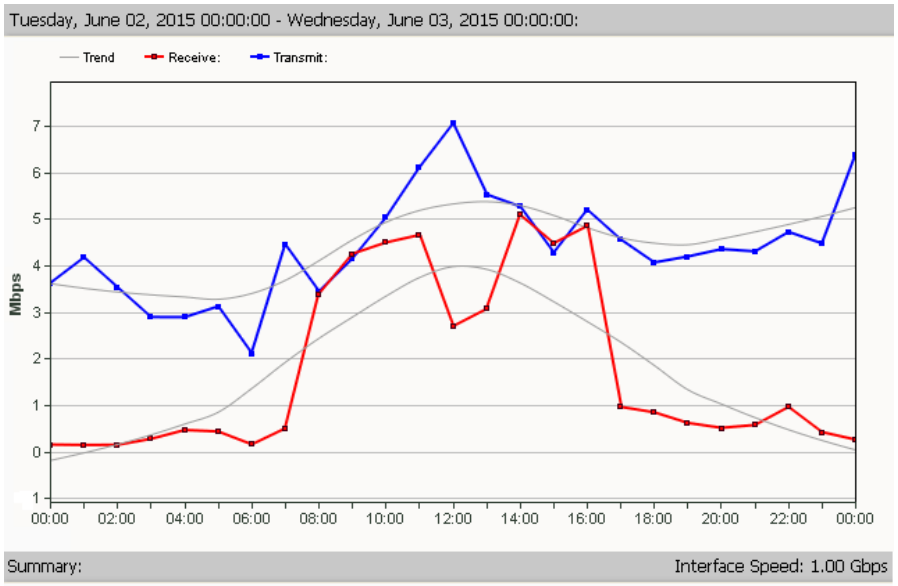
Los porcentajes de mayor consumo son reportados dentro de las horas de oficina, que comprende desde las 8:00 hasta 17:00, con un consumo máximo de transmisión de 12.11 Mbps y un máximo de recepción de 7.41 Mbps. Las figuras 3.113, 3.114, 3.115, 3.116 y 3.119 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 de cada día, en donde se puede evidenciar que los valores de transmisión y recepción varían durante todo el día y especialmente en horarios de oficina con la característica de que los valores de transmisión son mayores a la recepción. Las figuras 3.117 y 3.118 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 durante el fin de semana, en donde se puede evidenciar que los valores de transmisión y recepción presentan valores bajos. La figura 3.120 muestra el monitoreo realizado durante toda la semana, en donde se puede evidenciar el consumo diario.

Figura 3. 113 Consumo de ancho de banda lunes 01 al martes 02 de Junio



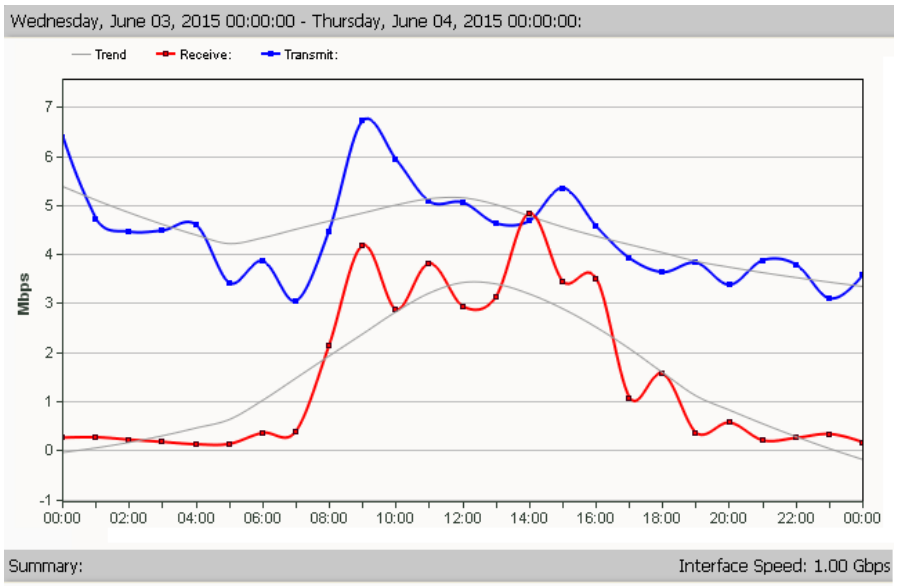
	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	108.73 Kbps	9.42 Mbps	1.61 Mbps	0.01 %	0.94 %	0.16 %
Transmit:	1.49 Mbps	12.22 Mbps	4.62 Mbps	0.15 %	1.22 %	0.46 %

Figura 3. 114 Consumo de ancho de banda martes 02 al miércoles 03 de Junio



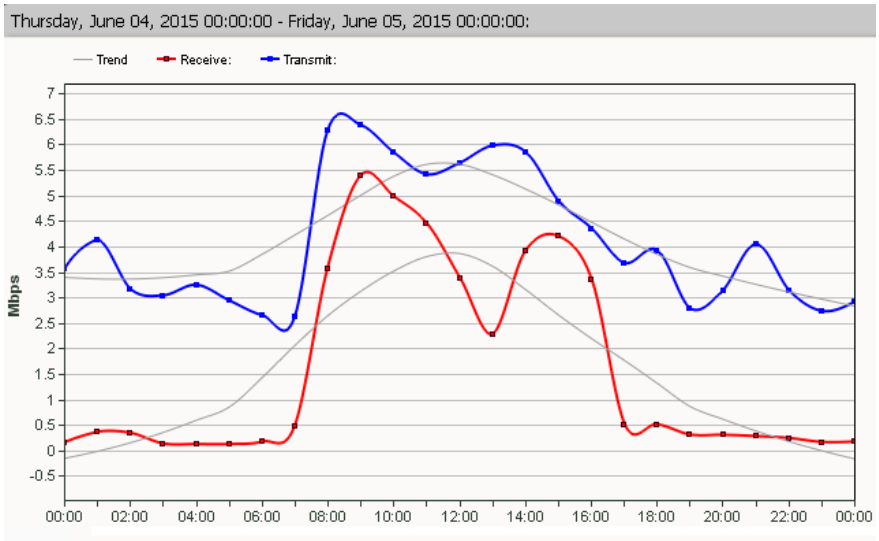
	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	110.17 Kbps	7.41 Mbps	1.77 Mbps	0.01 %	0.74 %	0.18 %
Transmit:	1.40 Mbps	7.68 Mbps	4.39 Mbps	0.14 %	0.77 %	0.44 %

Figura 3. 115 Consumo de ancho de banda miércoles 03 al jueves 04 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	113.92 Kbps	6.89 Mbps	1.49 Mbps	0.01 %	0.69 %	0.15 %
Transmit:	2.45 Mbps	7.80 Mbps	4.41 Mbps	0.24 %	0.78 %	0.44 %

Figura 3. 116 Consumo de ancho de banda jueves 04 al viernes 05 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	117.25 Kbps	5.93 Mbps	1.60 Mbps	0.01 %	0.59 %	0.16 %
Transmit:	2.25 Mbps	8.94 Mbps	4.09 Mbps	0.23 %	0.89 %	0.41 %

Figura 3. 117 Consumo de ancho de banda sábado 06 al domingo 07 de Junio

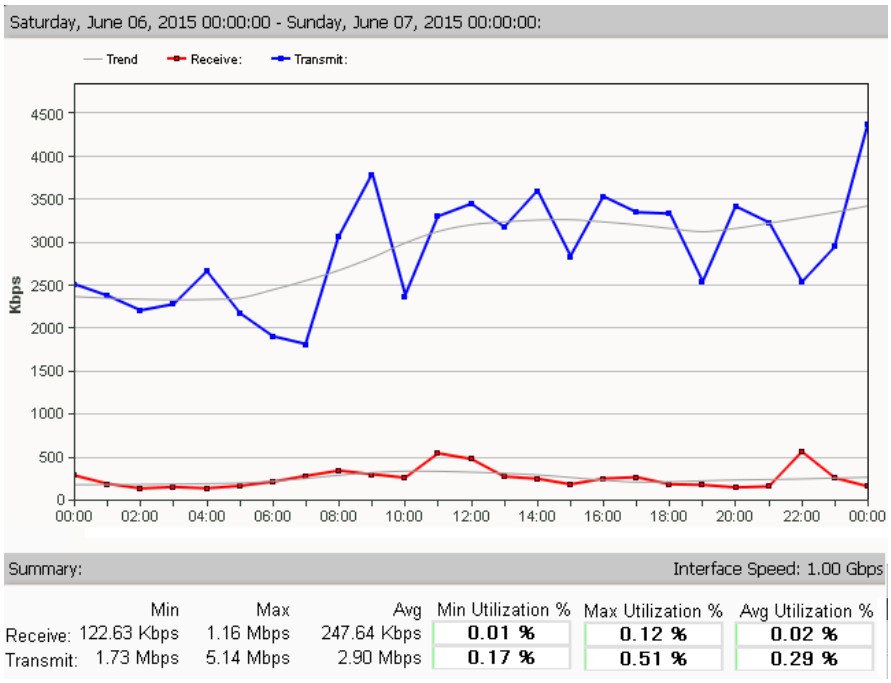


Figura 3. 118 Consumo de ancho de banda domingo 07 al lunes 08 de Junio

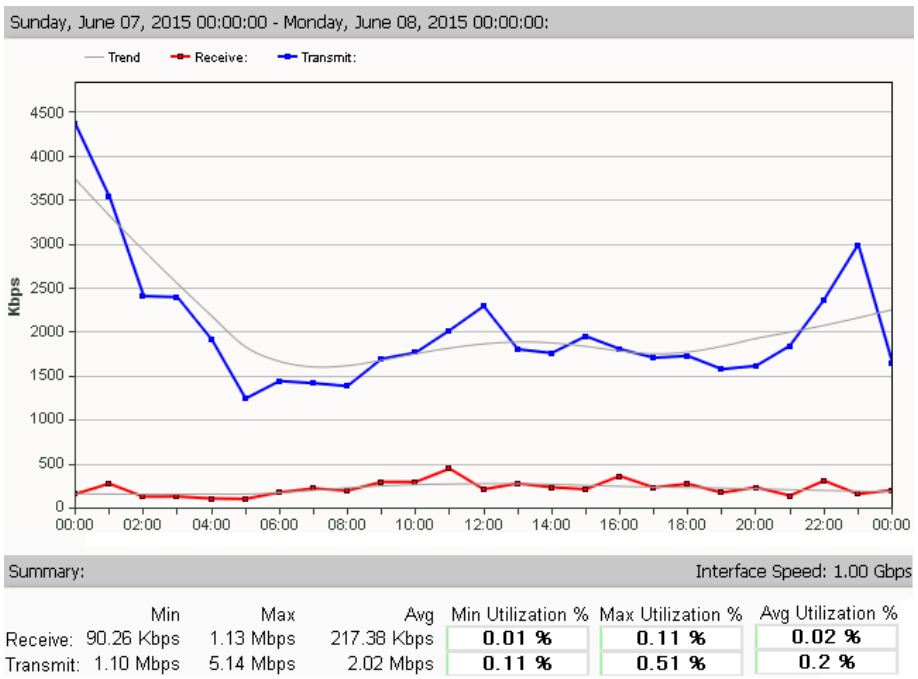


Figura 3. 119 Consumo de ancho de banda lunes 08 al martes 09 de Junio

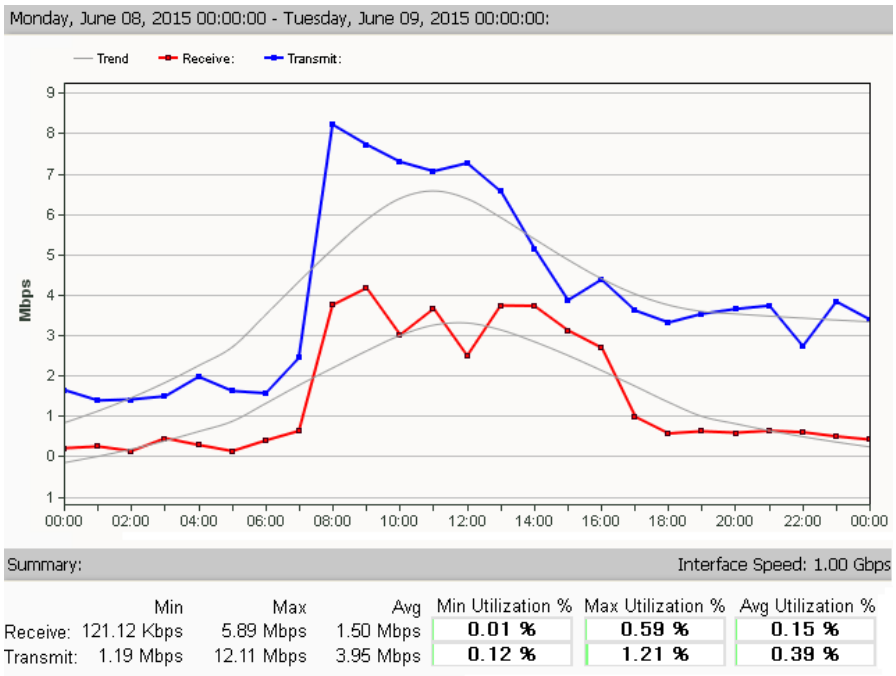
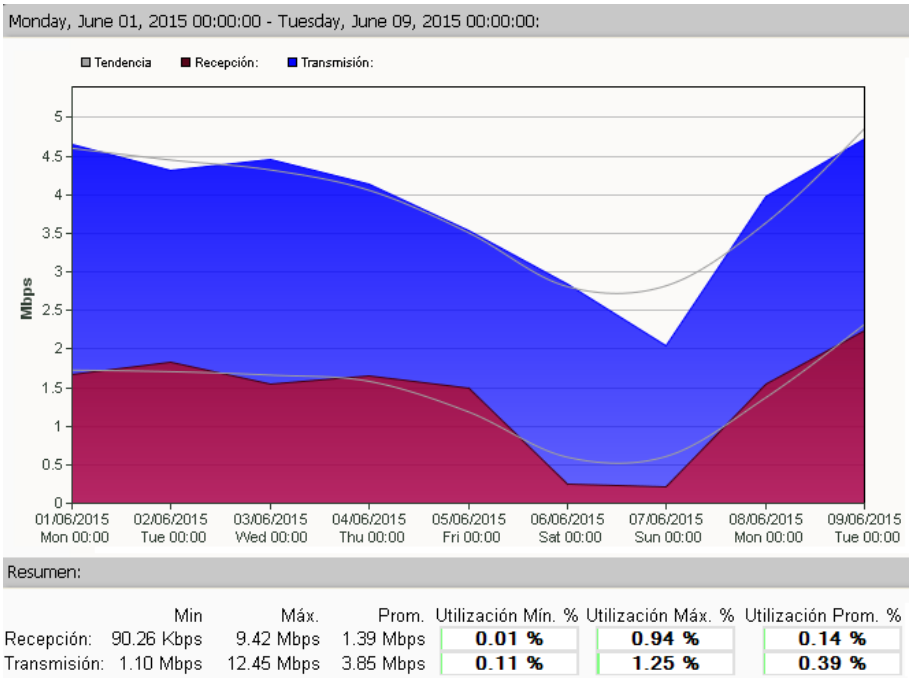


Figura 3. 120 Consumo de ancho de banda de la semana del lunes 01 al martes 09 de Junio



3.5.5.11 Enlace ROUTERFW - FIREWALL

El porcentaje de mayor consumo en cuanto a Transmisión se reporta a las 4:00 debido a una actualización realizada automáticamente. Con un consumo máximo de transmisión de 41.98 Mbps y un máximo de recepción de 9.74 Mbps. Las figuras 3.121, 3.122, 3.123, 3.124 y 3.127 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 de cada día, en donde se puede evidenciar que los valores de transmisión y recepción varían durante todo el día y especialmente en horarios de oficina. Las figuras 3.125 y 3.126 muestran el monitoreo realizado desde las 00:00 hasta las 23:59 durante el fin de semana, en donde se puede evidenciar que los valores de transmisión y recepción presentan valores bajos. La figura 3.128 muestra el monitoreo realizado durante toda la semana, en donde se puede evidenciar el consumo diario.

Figura 3. 121 Consumo de ancho de banda lunes 01 al martes 02 de Junio

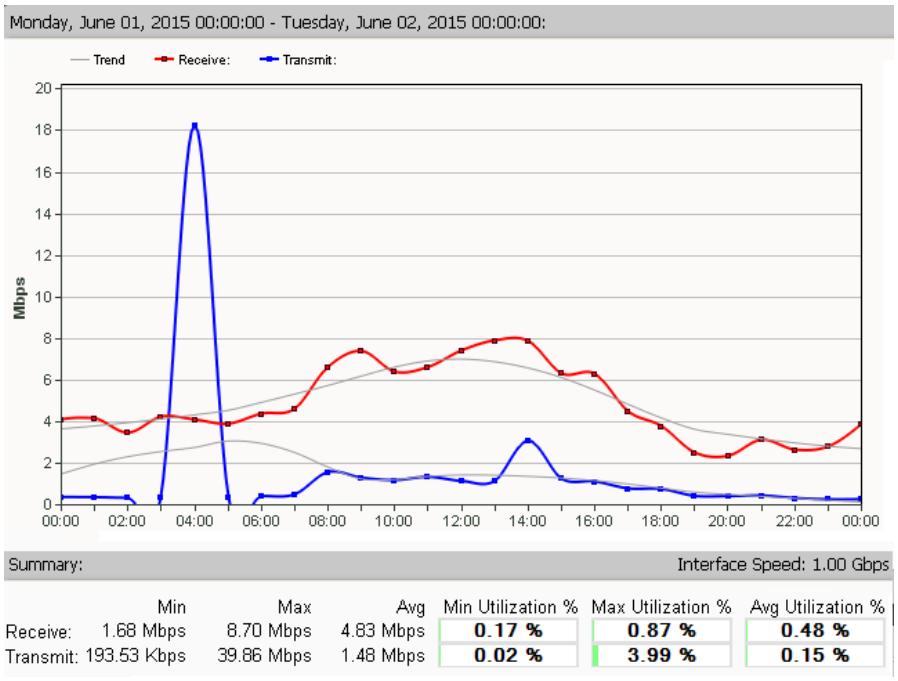


Figura 3. 122 Consumo de ancho de banda martes 02 al miércoles 03 de Junio

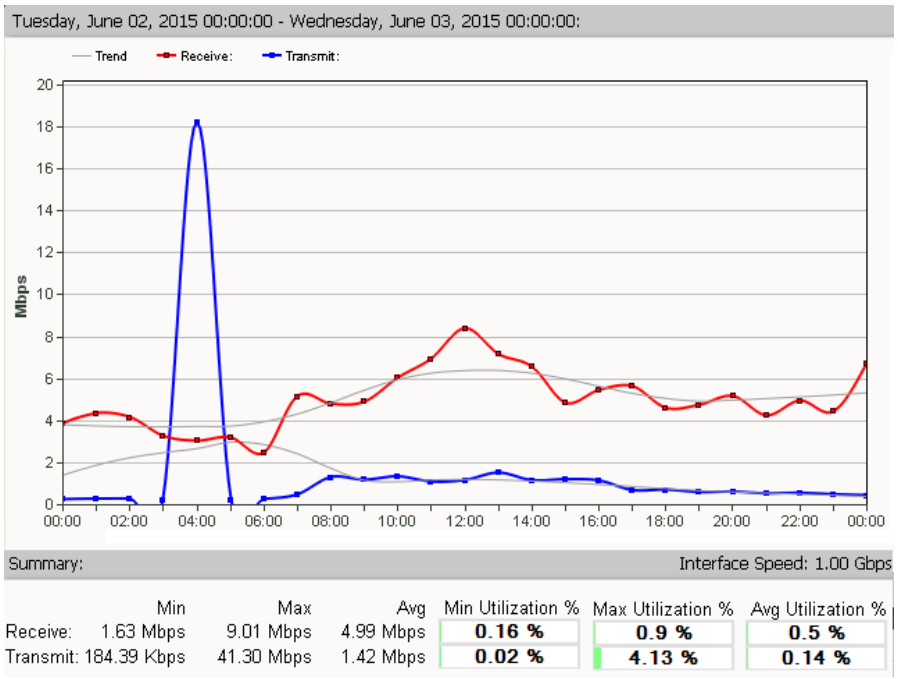


Figura 3. 123 Consumo de ancho de banda miércoles 03 al jueves 04 de Junio

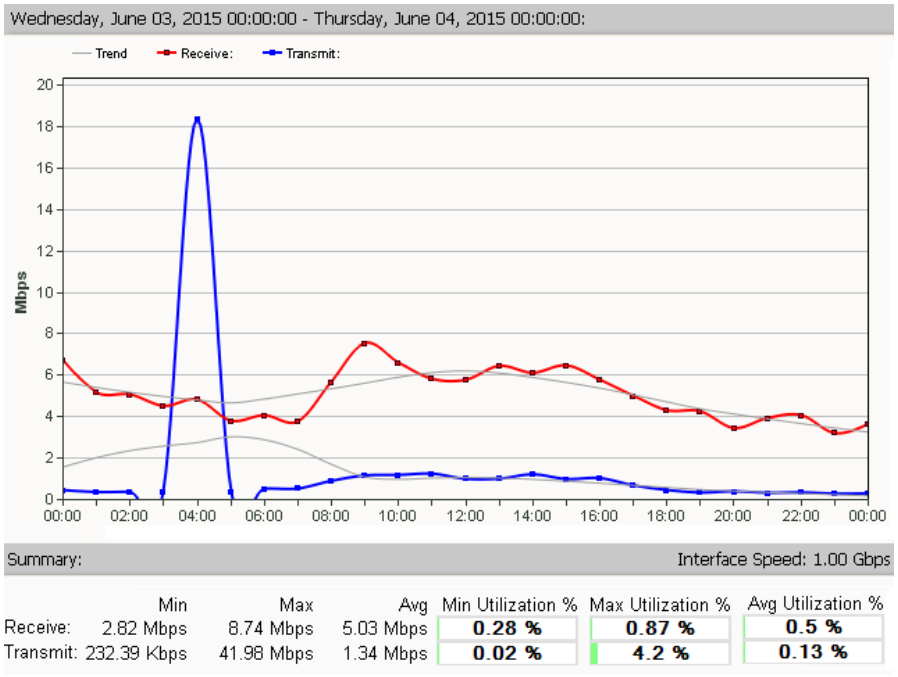


Figura 3. 124 Consumo de ancho de banda jueves 04 al viernes 05 de Junio

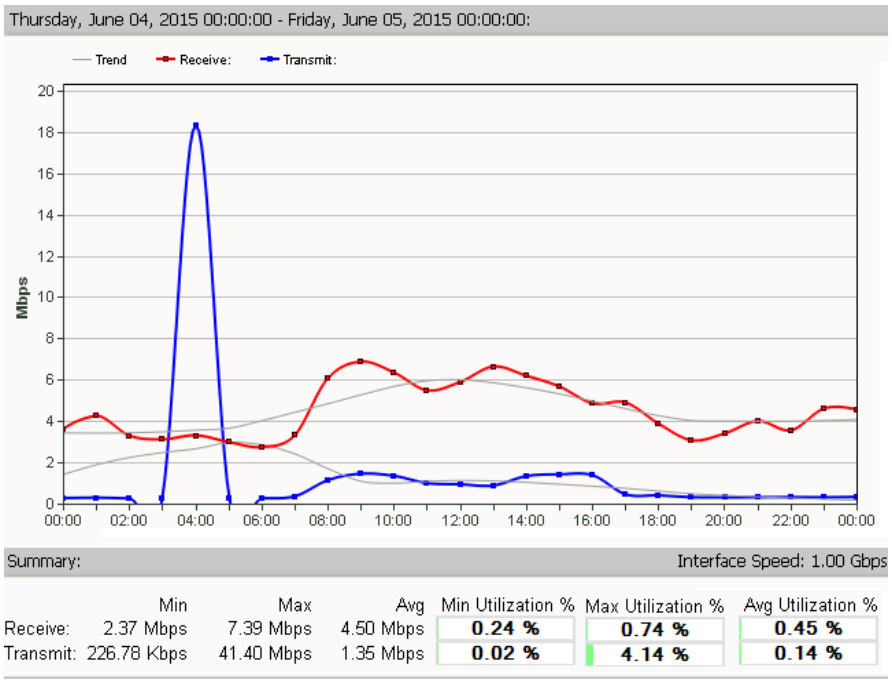


Figura 3. 125 Consumo de ancho de banda sábado 06 al domingo 07 de Junio

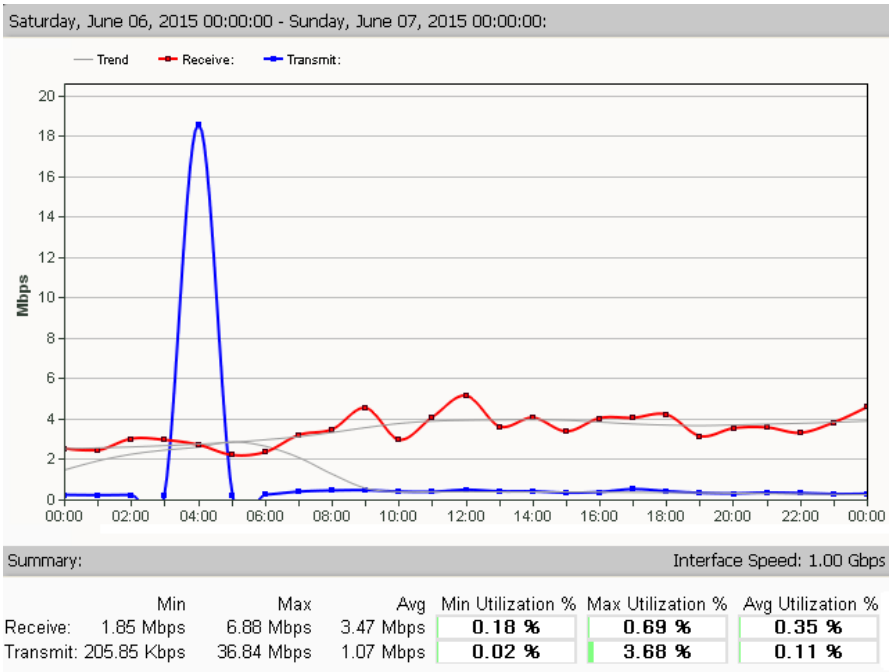
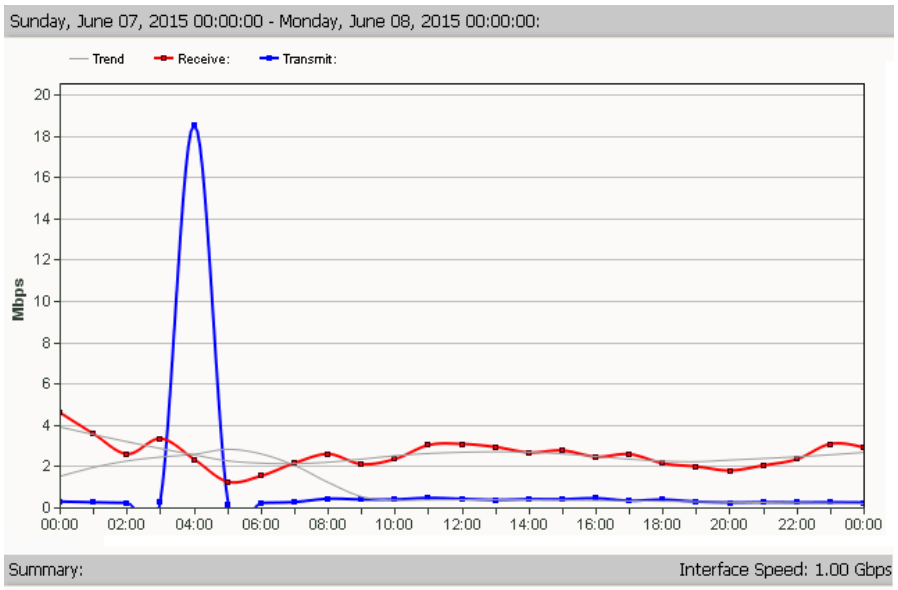
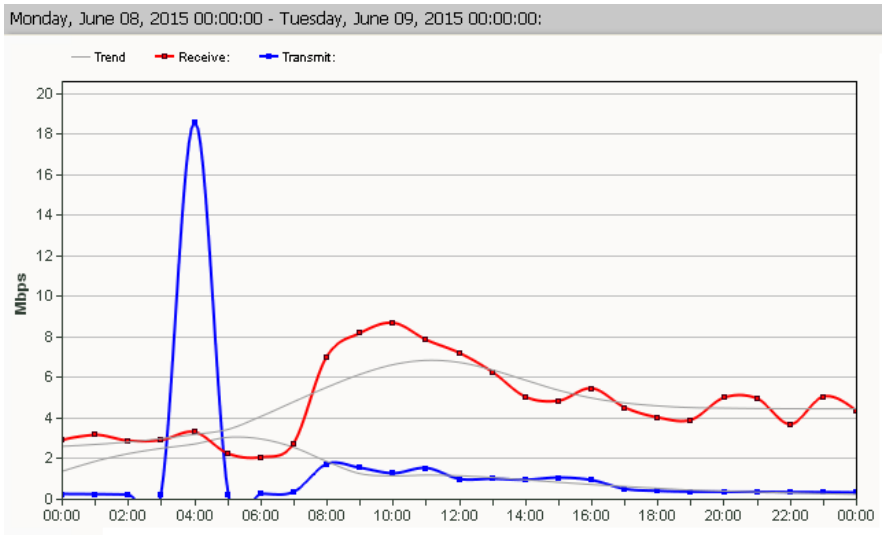


Figura 3. 126 Consumo de ancho de banda domingo 07 al lunes 08 de Junio



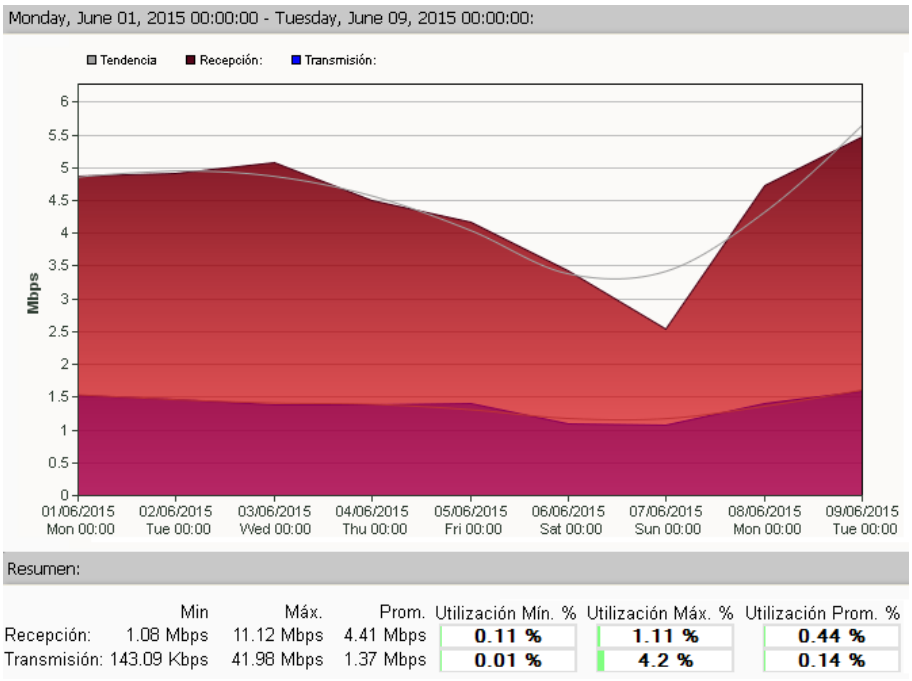
	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	1.08 Mbps	5.85 Mbps	2.56 Mbps	0.11 %	0.58 %	0.26 %
Transmit:	143.09 Kbps	33.83 Mbps	1.04 Mbps	0.01 %	3.38 %	0.1 %

Figura 3. 127 Consumo de ancho de banda lunes 08 al martes 09 de Junio



	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive:	1.52 Mbps	9.74 Mbps	4.71 Mbps	0.15 %	0.97 %	0.47 %
Transmit:	197.15 Kbps	31.89 Mbps	1.36 Mbps	0.02 %	3.19 %	0.14 %

Figura 3. 128 Consumo de ancho de banda de la semana del lunes 01 al martes 09 de Junio



Las siguientes tablas muestra los valores resumidos del consumo en Mbps (TX y RX) de los enlaces de mayor tráfico durante la semana:

Tabla 3. 16 Resumen de consumo (Mbps) TX - RX enlace CORE-SWDATACENTER

HORAS	Enlace CORE - SWDATACENTER											
	DÍAS											
	LUNES		MARTES		MIERCOLES		JUEVES		LUNES		PROMEDIO	
	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX
0:00	1	1	2	1	1	1	1	1	1	1	1	1
1:00	2	2	1	2	1	3	1	3	1	1	1	2
2:00	1	1	2	1	1	1	1	1	1	1	1	1
3:00	1	1	2	1	1	1	1	1	1	1	1	1
4:00	1	18	2	19	1	19	1	19	1	19	1	19
5:00	1	1	4	2	1	1	1	1	1	1	2	1
6:00	3	1	1	1	1	1	1	1	1	1	1	1
7:00	7	2	7	2	1	3	1	1	4	1	4	2
8:00	35	26	23	7	12	5	13	4	35	20	24	12
9:00	17	7	13	10	18	6	13	5	33	20	19	10
10:00	22	6	23	9	14	5	11	4	18	10	18	7
11:00	25	5	17	7	16	6	13	7	16	9	17	7
12:00	18	6	10	6	9	5	11	5	11	13	12	7
13:00	14	5	9	7	12	6	13	5	11	7	12	6
14:00	18	7	14	7	9	4	19	6	15	6	15	6
15:00	20	5	12	5	14	6	11	5	8	5	13	5
16:00	14	5	10	7	9	4	11	6	8	4	10	5
17:00	5	4	2	1	2	2	5	1	5	2	4	2
18:00	3	1	1	1	1	1	1	1	1	1	1	1
19:00	1	1	1	1	1	1	1	1	1	1	1	1
20:00	2	1	1	1	1	1	1	1	1	1	1	1
21:00	1	1	1	1	1	1	1	1	1	1	1	1
22:00	2	1	1	1	1	1	1	1	1	1	1	1
23:00	4	1	1	1	1	1	1	1	1	1	2	1

Tabla 3. 17 Resumen de consumo (Mbps) TX - RX enlace CORE-SWTECNICA

HORAS	Enlace CORE - SWTECNICA											
	DÍAS											
	LUNES		MARTES		MIERCOLES		JUEVES		LUNES		PROMEDIO	
	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX
0:00	1	1	0,1	O,1	0,2	O,1	0,2	O,1	O,1	O,1	0	1
1:00	1	1	0,1	0,1	0,3	0,1	0,2	0,1	0,1	0,1	0	0
2:00	1	1	0,2	0,1	0,2	0,1	0,2	0,1	0,1	0,1	0	0
3:00	1	1	0,3	0,1	0,1	0,1	0,2	0,1	0,1	0,1	0	0
4:00	1	1	0,4	0,1	0,1	0,1	0,2	0,1	0,1	0,1	0	0
5:00	1	1	0,4	0,1	0,1	0,1	0,2	0,1	0,1	0,1	0	0
6:00	1	1	0,1	0,1	0,1	0,1	0,2	0,1	0,1	0,1	0	0
7:00	3	1	2	0,2	0,4	0,3	0,3	0,3	0,1	0,1	1	0
8:00	3	3	2,3	1,4	3,5	1	2,4	2,1	2,1	0,2	3	2
9:00	2	1	2,4	1,5	1,2	0,8	1,6	1,3	0,2	0,1	1	1
10:00	2	2	1	0,6	1,3	1,1	2,2	1	0,2	0,2	1	1
11:00	2	2	1,8	1,4	1,7	1,3	2,2	1,1	0,2	0,2	2	1
12:00	2	6	2,6	3,4	1,4	3,3	1,3	0,9	0,2	0,3	2	3
13:00	2	2	1,3	0,7	1,7	1	1,4	1,4	0,2	0,1	1	1
14:00	3	3	1,4	0,9	1,9	1,4	1,6	1,3	0,6	0,2	2	1
15:00	2	2	1,3	0,8	1,1	0,9	1,7	1,3	0,2	0,2	1	1
16:00	2	2	1	0,7	0,8	0,8	1	0,6	0,2	1	1	1
17:00	2	1	0,2	0,1	0,4	0,1	0,5	0,6	0,1	0,1	1	0
18:00	1	1	0,3	0,1	0,2	0,1	0,2	0,1	0,1	0,1	0	0
19:00	1	1	0,2	0,1	0,2	0,1	0,2	0,1	0,1	0,1	0	0
20:00	1	1	0,2	0,1	0,2	0,1	0,2	0,1	0,1	0,1	0	0
21:00	1	1	0,3	0,1	0,2	0,1	0,2	0,1	0,1	0,1	0	0
22:00	1	1	0,2	0,1	0,2	0,1	0,2	0,1	0,1	0,1	0	0
23:00	1	1	0,1	0,1	0,2	0,1	0,2	0,1	0,1	0,1	0	0

Tabla 3. 18 Resumen de consumo (Mbps) TX - RX enlace SWDATACENTER - SWQUITO

HORAS	Enlace SWDATACENTER - SWQUITO											
	DÍAS											
	LUNES		MARTES		MIERCOLES		JUEVES		LUNES		PROMEDIO	
	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX
0:00	1	1	2	1	1	1	1	1	1	1	1	1
1:00	1	2	1	2	1	2	1	2	1	1	1	2
2:00	1	1	2	1	1	1	1	1	1	1	1	1
3:00	1	1	2	1	1	1	1	1	1	1	1	1
4:00	1	18	2	18	1	18	1	19	1	18	4	18
5:00	1	1	2	2	1	1	1	1	1	1	1	1
6:00	2	1	1	1	1	1	1	1	1	1	1	1
7:00	1	1	3	2	1	1	1	1	2	1	1	1
8:00	25	20	15	3	6	1	9	2	26	14	14	8
9:00	8	4	4	3	12	2	9	2	25	15	11	5
10:00	18	4	20	8	5	2	6	2	16	10	11	5
11:00	20	4	10	4	13	2	9	5	10	6	11	4
12:00	16	4	4	3	5	2	5	2	6	10	7	4
13:00	10	3	3	4	7	2	9	3	3	3	7	3
14:00	13	5	8	5	5	2	14	4	3	2	8	4
15:00	14	3	8	1	9	4	6	2	3	2	7	2
16:00	13	4	7	5	4	2	5	2	3	2	6	3
17:00	5	1	1	1	3	1	4	1	1	1	3	1
18:00	3	1	1	1	1	1	1	1	1	1	1	1
19:00	1	1	1	1	1	1	1	1	1	1	1	1
20:00	3	1	1	1	1	1	1	1	1	1	1	1
21:00	1	1	1	1	1	1	1	1	1	1	1	1
22:00	3	1	1	1	1	1	1	1	1	1	1	1
23:00	3	1	1	1	1	1	1	1	1	1	1	1

Tabla 3. 19 Resumen de consumo (Mbps) TX - RX enlace ROUTER GUANGOPOLO - ROUTER QUITO

HORAS	Enlace ROUTER GUANGOPOLO - ROUTER QUITO											
	DÍAS											
	LUNES		MARTES		MIERCOLES		JUEVES		LUNES		PROMEDIO	
	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX
0:00	4	0,2	3,7	0,1	6,2	0,2	3,5	0,2	1,5	0,2	4	0
1:00	4	0,2	4,1	0,1	5,5	0,2	4,2	0,5	1,5	0,2	4	0
2:00	3	0,2	3,5	0,2	5,5	0,1	3,2	0,5	1,5	0,1	3	0
3:00	4	0,2	2,9	0,1	5,5	0,1	3	0,1	1,5	0,4	3	0
4:00	4	0,2	2,9	0,5	5,6	0,1	3,2	0,1	2	0,5	4	0
5:00	3	0,2	3,1	0,5	3,5	0,1	3	0,1	1,5	0,1	3	0
6:00	4	0,2	2,1	0,1	3,8	0,5	2,6	0,1	1,5	0,5	3	0
7:00	4	0,5	4,5	0,5	3	0,5	2,6	0,5	2,5	0,8	3	1
8:00	8	3,5	3,5	3,5	4,5	2,1	6,3	3,6	8	3,8	6	3
9:00	7	4,1	4,1	4,5	6,8	4,2	6,4	5,5	7,9	4,2	6	5
10:00	7,5	3,5	5	4,6	6	3	5,8	5,1	7,4	3	6	4
11:00	6	4,1	6,1	4,8	5	4	5,5	4,6	7	3,8	6	4
12:00	7,1	3,5	7	2,9	5	3	5,6	3,5	7,1	2,8	6	3
13:00	7,1	3,1	5,5	3,1	4,7	3,2	6	2,5	6,5	3,9	6	3
14:00	6,9	5	5,2	5,1	4,7	5	5,8	4	5,1	4	6	5
15:00	6	3,2	4,2	4,5	5,5	3,5	5	4,4	4	3,1	5	4
16:00	5,9	5	5,2	5,1	4,6	3,5	4,9	3,5	4,2	3	5	4
17:00	3,8	1,5	4,5	1	3,9	1	3,6	0,5	3,8	1	4	1
18:00	3,4	0,9	4	1	3,7	1,7	4	0,5	3,2	0,6	4	1
19:00	2,5	0,5	4,2	0,8	3,8	0,5	2,7	0,4	3,2	0,6	3	1
20:00	2	0,5	4,3	0,5	3,4	0,7	3,2	0,4	3,7	0,6	3	1
21:00	2,6	0,5	4,3	0,5	3,8	0,2	4	0,4	3,8	0,6	4	0
22:00	2,5	0,5	4,7	1	3,7	0,3	3,2	0,4	2,8	0,6	3	1
23:00	2,6	0,5	4,5	0,5	3,1	0,3	2,6	0,3	3,9	0,5	3	0

Tabla 3. 20 Resumen de consumo (Mbps) TX - RX enlace ROUTER QUITO - FIREWALL

HORAS	Enlace ROUTER QUITO - FIREWALL											
	DÍAS											
	LUNES		MARTES		MIERCOLES		JUEVES		LUNES		PROMEDIO	
	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX
0:00	4	0,2	3,7	0,1	6,5	0,2	3,5	0,2	1,9	0,2	4	0
1:00	4	0,2	4	0,1	4,7	0,2	4	0,4	1,5	0,2	4	0
2:00	3,2	0,1	3,5	0,1	4,5	0,2	3,1	0,4	1,5	0,1	3	0
3:00	4	0,1	3	0,4	4,5	0,1	3	0,1	1,5	0,5	3	0
4:00	4	0,1	3	0,5	4,6	0,1	3,2	0,1	2	0,3	3	0
5:00	3,8	0,1	3,1	0,5	3,5	0,1	3	0,1	1,5	0,2	3	0
6:00	4	0,2	2	0,1	3,8	0,3	2,6	0,1	1,5	0,5	3	0
7:00	4	0,5	4,5	0,5	3	0,3	2,6	0,5	2,5	0,7	3	1
8:00	8	3,2	3,5	3,5	4,5	2,1	6,3	3,5	8	3,9	6	3
9:00	7	4,1	4,1	4,1	6,8	4,1	6,4	5,5	7,8	4,1	6	4
10:00	7,5	3,2	5	4,5	6	3	5,9	5	7,2	3	6	4
11:00	6	4	6	4,7	5	3,8	5,5	4,5	7	3,8	6	4
12:00	7	3,3	7	2,8	5	3	5,6	3,5	7,2	2,5	6	3
13:00	7,1	3	5,5	3	4,5	3	6	2,4	6,6	3,8	6	3
14:00	7	5	5,4	5	4,5	4,9	5,9	4	5,1	3,8	6	5
15:00	6	3,1	4,1	4,5	5,2	3,5	4,9	4,2	4	3	5	4
16:00	5,9	5	5,1	4,8	4,5	3,5	4,4	3,4	4,3	2,8	5	4
17:00	3,8	1,5	4,5	1	4	1	3,6	0,5	3,5	1	4	1
18:00	3,4	0,9	4	0,9	3,5	1,5	4	0,5	3,3	0,5	4	1
19:00	2,5	0,5	4,1	0,5	3,8	0,2	2,6	0,4	3,5	0,5	3	0
20:00	2	0,5	4,2	0,5	3,4	0,5	3,1	0,4	3,6	0,5	3	0
21:00	2,8	0,5	4,2	0,5	3,8	0,1	4	0,4	3,8	0,5	4	0
22:00	2,5	0,2	4,6	1	3,7	0,2	3,1	0,3	2,9	0,5	3	0
23:00	2,8	0,3	4,5	0,5	3,1	0,2	2,6	0,2	3,9	0,5	3	0

Tabla 3. 21 Resumen de consumo (Mbps) TX - RX enlace ROUTERFW - FIREWALL

HORAS	Enlace ROUTERFW - FIREWALL											
	DÍAS											
	LUNES		MARTES		MIERCOLES		JUEVES		LUNES		PROMEDIO	
	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX
0:00	0,5	4	0,5	4	0,5	6,5	0,5	4	0,5	3	1	4
1:00	0,5	4	0,5	4,5	0,5	5	0,5	4,5	0,5	3	1	4
2:00	0,5	3	0,5	4,5	0,5	5	0,5	3	0,5	3	1	4
3:00	0,5	4	0,5	3	0,5	4,5	0,5	3	0,5	3	1	4
4:00	18	4	18	3	18	5	18	3,5	18	3,5	18	4
5:00	0,5	4	0,5	3	0,5	4	0,5	3	0,5	2	1	3
6:00	0,5	4,5	0,5	2,5	0,5	4	0,5	3	0,5	2	1	3
7:00	0,5	5	0,5	5	0,5	4	0,5	3,5	0,5	3	1	4
8:00	1,5	6,5	1	5	1	5,5	1	6	2	7	1	6
9:00	1,5	7	1	5	1	7,5	1,5	6,5	1,5	8	1	7
10:00	1,5	6,5	1	6	1	6,5	1,5	6	1	8,5	1	7
11:00	1,5	6,5	1	7	1	6	1	5,5	1,5	8	1	7
12:00	1,5	7	1	8	1	6	1	6	1	7	1	7
13:00	1,5	8	1,5	7	1	6,5	1	6,5	1	6	1	7
14:00	3	8	1	6,5	1,5	6	1,5	5	1	5	2	6
15:00	1,5	6	1	5	1	6,5	1,5	6	1	5	1	6
16:00	1,5	6	1	5,5	1	6	1,5	5	1	5,5	1	6
17:00	1	4	1	6	1	5	0,5	5	0,5	4,5	1	5
18:00	0,5	4	0,5	4,5	0,5	4	0,5	4	0,5	4	1	4
19:00	0,5	1	0,5	4,5	0,5	4	0,5	3	0,5	4	1	3
20:00	0,5	1	0,5	5	0,5	3	0,5	3,5	0,5	5	1	4
21:00	0,5	3	0,5	4,5	0,5	4	0,5	4	0,5	5	1	4
22:00	0,5	3	0,5	5	0,5	4	0,5	3,5	0,5	4	1	4
23:00	0,5	3	0,5	4,5	0,5	3	0,5	4,5	0,5	5	1	4

Tabla 3. 22 Resumen de consumo (Mbps) TX - RX enlace CORE - ROUTER GUANGOPOLO

HORAS	Enlace CORE - ROUTER GUANGOPOLO											
	DÍAS											
	LUNES		MARTES		MIERCOLES		JUEVES		LUNES		PROMEDIO	
	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX
0:00	4	0,5	3,8	0,1	6	0,4	3,35	0,3	1,8	0,2	4	0
1:00	4	0,1	4,1	0,1	5	0,2	4	0,5	1,5	0,2	4	0
2:00	3,5	0,1	3,5	0,1	4,5	0,2	3,1	0,4	1,5	0,1	3	0
3:00	4	0,1	3	0,2	4,5	0,1	3	0,2	1,5	0,5	3	0
4:00	4	0,1	3	0,5	4,6	0,1	3,4	0,2	2	0,4	3	0
5:00	3,9	0,1	3,1	0,5	3,5	0,1	3	0,2	1,5	0,2	3	0
6:00	4,1	0,5	2,1	0,2	3,9	0,5	2,6	0,2	1,5	0,5	3	0
7:00	4	0,7	4,5	0,6	3	0,5	3	0,6	2,5	0,7	3	1
8:00	8,5	4	3,8	3,5	4,8	2,5	6,4	4	8,2	4	6	4
9:00	7	4,4	4	4,5	6,8	4,5	6,5	5,6	7,9	4,5	6	5
10:00	7,5	3,5	5	4,6	6	3,1	6	5,2	7,4	3,3	6	4
11:00	6	4,5	6	5	5	4,1	5,5	4,6	7	4	6	4
12:00	7,2	3,5	7,2	3,5	5,1	3	5,7	3,5	7,2	2,8	6	3
13:00	7,1	3,6	6	3	4,5	3,5	6	2,5	6,5	4	6	3
14:00	7	5	5,5	5,1	4,7	5,2	6	4,4	5,1	4	6	5
15:00	6	3,9	4,3	4,9	5,5	3,7	4,7	4,5	4	3,4	5	4
16:00	6	5	5	5,5	4,5	3,7	4,5	3,5	4,5	3	5	4
17:00	3,9	1,5	4,9	1,3	4	1,4	3,6	0,6	3,5	1	4	1
18:00	3,4	1	4	1	3,5	1,4	4	0,5	3,2	0,8	4	1
19:00	2,5	0,5	4,1	0,8	4	0,5	2,6	0,4	3,5	0,8	3	1
20:00	2	0,5	4,2	0,5	3,2	0,7	3,4	0,4	3,7	0,8	3	1
21:00	2,7	0,5	4,2	0,5	4	0,3	4	0,4	3,8	0,8	4	1
22:00	2,5	0,5	4,8	1	3,8	0,4	3	0,4	2,9	0,8	3	1
23:00	2,8	0,5	4,5	0,5	3	0,5	2,4	0,2	4	0,8	3	1

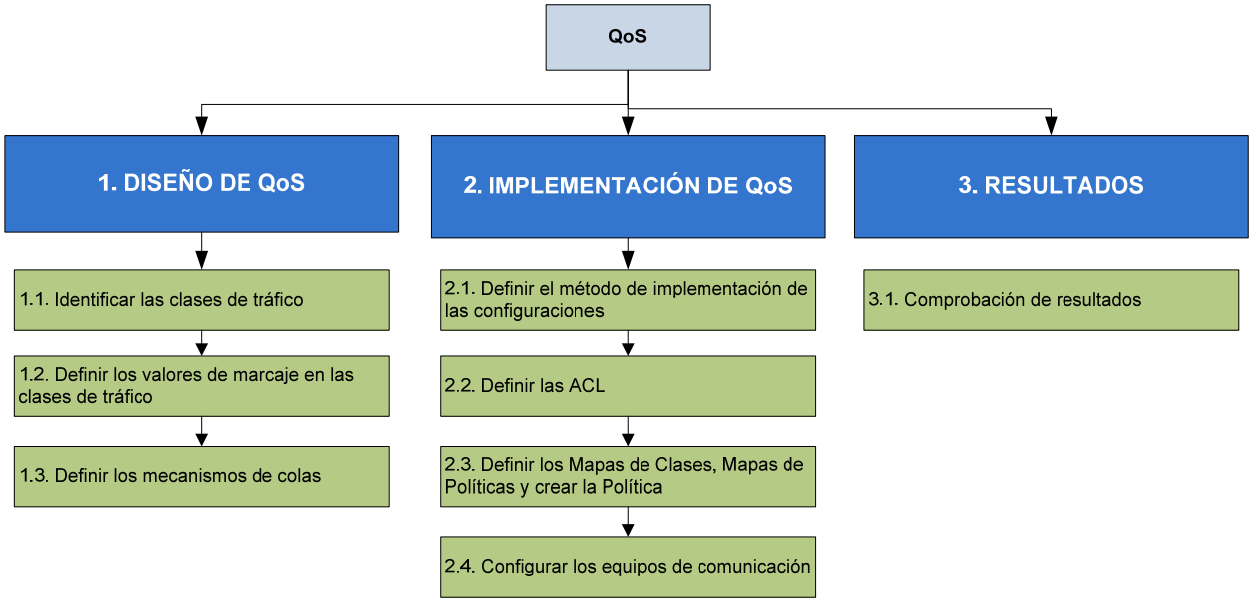
CAPÍTULO 4

DISEÑO, IMPLEMENTACIÓN Y RESULTADOS

4.1 Esquema de Diseño e Implementación

Se define a continuación un esquema de trabajo para la implementación y configuración de QoS, que involucra la identificación de los requerimientos y la selección de los distintos métodos para la clasificación, marcaje y control de congestión.

Figura 4. 1 Esquema de Diseño e Implementación



4.1.1 Diseño de QoS

4.1.1.1 Identificación de las clases de tráfico

Con el análisis realizado en el capítulo 3 del tráfico generado dentro de la Unidad de Negocios Termopichincha, se puede evidenciar que los horarios donde presenta mayor flujo de tráfico están entre 8:00 y las 17:00, en donde, la hora pico están comprendida entre las 8:00 y las 9:00, las horas de mayor tráfico está comprendida entre las 9:00 y las 11:00, como también

durante las 14:00, el tráfico moderado está comprendida entre las 12:00 y 13:00, como también entre las 15:00 hasta las 17:00. El flujo de tráfico se disminuye entre las 17:00 y las 24:00; 00:00 y las 7:00. Adicionalmente se evidencia que el día con mayor tráfico durante la semana es el Lunes (primer día de la semana). Es importante identificar que el tráfico generado en estos horarios es de gran importancias para el negocio debido a la importancia de su contenido.

La tabla 4.1 y 4.2, y la figura 4.1 presenta la información resumida de los consumos generados durante la semana de evaluación de los diferentes enlaces, evidenciando el día de mayor consumo y la hora pico.

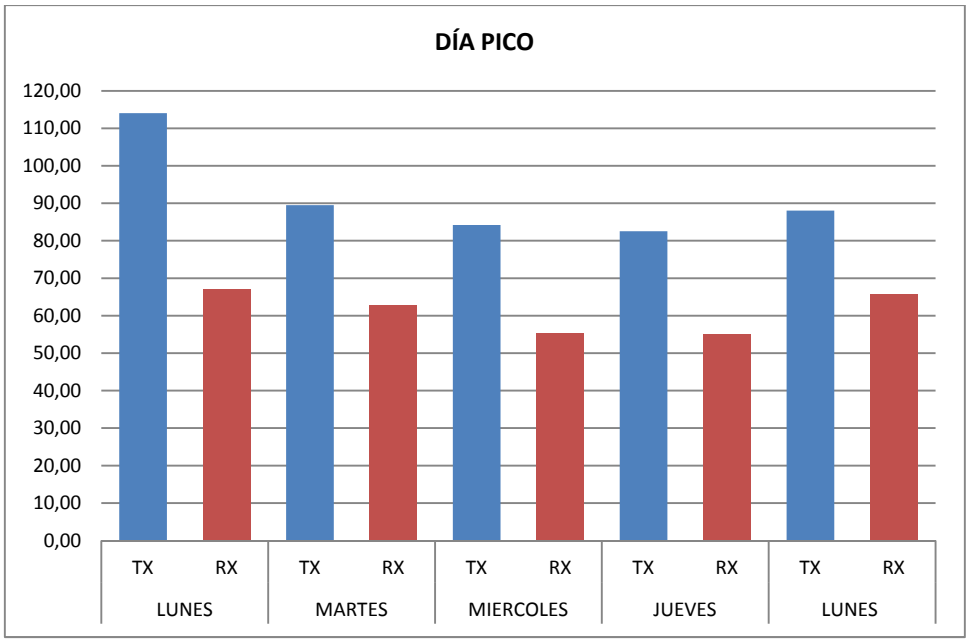
Tabla 4. 1 Resumen de consumo en Mbps de los Enlaces

	LUNES		MARTES		MIERCOLES		JUEVES		LUNES	
ENLACES	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX
Enlace CORE - SWDATACENTER	218	109	160	101	129	85	134	82	177	128
Enlace CORE - SWTECNICA	38	38	20,2	12,9	17,7	13,2	18,8	13,1	5,5	3,9
ROUTER GPO-UIO	110,9	41,8	103,1	45,5	110,8	38	99,9	41,7	95,1	38,9
ROUTER QUITO - FIREWALL	112,3	39,8	102,6	44,1	106,4	36,1	98,9	40,6	95,6	37,4
Enlace ROUTERFW - FIREWALL	40,5	113	35	118,5	35	121,5	36,5	107,5	36	114
Enlace CORE - ROUTER GUANGOPOLO	113,6	44,6	104,6	47,5	107,4	40,6	99,75	43,3	96,2	41,6
Enlace SWDATACENTER - SWQUITO	165	84	101	71	83	52	90	58	111	96
PROMEDIO	**114,04**	**67,17**	**89,50**	**62,93**	**84,19**	**55,20**	**82,55**	**55,17**	**88,06**	**65,69**

Tabla 4. 2 Horas identificadas

HORA PICO	8:00
HORAS MAYOR TRÁFICO	9:00
	10:00
	11:00
HORA TRÁFICO MODERADO	12:00
	13:00
HORAS MAYOR TRÁFICO	14:00
HORA TRÁFICO MODERADO	15:00
	16:00
	17:00

Figura 4. 2 Gráfica de consumo en Mbps de los Enlaces



Según la revisión realizada con el área de TIC y tomando en cuenta el día y las horas pico, se han determinado las clases que se manejarán durante el diseño de calidad de servicio.

- Clase de Voz y Video
- Clase de Servicios de Prioridad Alta
- Clase de Servicios de Prioridad Media
- Clase de Servicios de Prioridad Baja
- Clase por Defecto

4.1.1.1.1 Requerimientos de la Clase Voz y Video

En el caso de la voz y video se ha identificado que los requerimientos están enfocados en la eliminación de los 3 problemas más frecuentes con este tipo de tráfico, las cuales son: la perdida de paquetes, la latencia y el jitter, que provocan que una conversación sea entrecortada y se degrade durante su transcurso. La Tabla 4.3 presenta los parámetros que se deben cumplir para mantener una calidad alta en cuanto a la voz y video.

Tabla 4. 3 Parámetros de calidad VoIP

Parámetros	Valor
Pérdida de Paquetes	<3%
Latencia	<100ms
Jitter	<20ms

En cuanto a su ancho de banda, una comunicación de videoconferencia mediante los equipos Polycom requieren un mínimo de 400 kbps (entre 2 usuarios) y un máximo de 800 kbps (más de 2 usuarios). Estos datos fueron proporcionados por el mismo sistema de videoconferencia. La telefonía IP (Siemens), el ancho de banda depende del número de llamadas simultaneas que se realicen, pero el valor mínimo es de 64 kbps (codec G.711) y un máximo de 100 kbps.

Por sus requerimientos, es la clase con mayor prioridad para ser considerada dentro de la implementación de QoS. Como se muestra la tabla 4.4, de la información recolectada en el capitulo anterior, podemos determinar que protocolos y puertos pertenecen dentro de esta clase.

Tabla 4. 4 Protocolos y puertos Clase Voz y Video

	Protocolos	Puertos
Clase Voz y Video	H323	1719
	HTTP	80
	HTTPS	443
	SIP	5060
	TCP	1718 - 1731
		3230
		5001
		1718 - 1731

	UDP	5001
	H323	1720
	RTP	

4.1.1.1.2 Requerimientos de la Clase de Servicios de Prioridad Alta

En el caso de los servicios con prioridad alta, se ha identificado que los requerimientos están enfocados en la eliminación del retardo en la entrega de la información, ya que podría afectar directamente a los servicios y evitar cualquier pérdida de información durante su trayectoria. A continuación se muestran los servicios críticos identificados.

- Sistema Financiero IFS
- Scada
- Aplicaciones Lotus
- Correo Electrónico
- Base de Datos
- Evolution

Por sus requerimientos, es importante que sea considerada dentro de la implementación de QoS. Como se muestra la tabla 4.5, de la información recolectada en el capitulo anterior, podemos determinar que protocolos y puertos pertenecen dentro de esta clase.

En cuanto al ancho de banda, el Sistema Financiero IFS requiere de un mínimo de 1000 kbps y un máximo de 1600 kbps, pero a finales del mes es posible que este valor incremente debido a los cierres de cada departamento. Correo Electrónico y Aplicaciones Lotus se requiere de un mínimo de 300 kbps y un máximo de 500 kbps. Scada se requiere de un mínimo de 10 kbps y un máximo de 50 kbps debido a que son archivos planos de tamaño mínimo. Evolution se requiere

de un mínimo de 100 kbps y un máximo de 150 kbps. Bases de Datos se requiere de un mínimo de 100 kbps y un máximo de 200 kbps.

Tabla 4. 5 Protocolos y puertos de la clase de prioridad alta

Servicio	Protocolo	Puerto
IFS (Sistema Financiero Integrado)	TCP	58080
		59080
		60080
		8093
SCADA	HTTP	80
	ModBus	502
	TCP	10001
		4050
		7700
		7701
		7717
		7779
		7800
		7801
		433
		50610
		49333
	DNP3	20000
Aplicaciones Lotus	HTTP	80
	HTTPS	443

	lotus	1352
	Sametime	1533
Correo Electrónico	imap	143
	imap-ssl	993
	lotus	1352
	pop-3	110
	smtp	25
Base de Datos	MS-SQL-Server	1433
	MS-SQL-Monitor	1434
	sqlnet	1521, 1525, 1526
	Sqlserver	
	oraclenames	
Evolution	HTTP	80

4.1.1.1.3 Requerimientos de la Clase de Servicios de Prioridad Media

En el caso de los servicios con prioridad media se ha identificado que los requerimientos están enfocados en la comunicación permanente pero podría existir perdida en su entrega. Estos servicios se encuentran trabajando permanentemente dentro de la red, generando tráfico para sincronización, comunicación, servicios de red y actualización. A continuación se muestran los servicios de prioridad media identificados.

- Directorio Activo
- Asignaciones de direcciones por DHCP
- DNS
- Symantec Antivirus

- Escritorios Remotos
- Carpetas Compartidas

En cuanto a su ancho de banda, son valores casi constantes que podrían variar debido a los servicios de Escritorio Remoto o Carpetas Compartidas. Podríamos definir que el valor mínimo requerido es de 50 kbps y un máximo de 400 kbps.

Por sus requerimientos es importante que sea considerada dentro de la implementación de QoS. Como se muestra la tabla 4.6 de la información recolectada en el capitulo anterior podemos determinar que protocolos y puertos pertenecen dentro de esta clase.

Tabla 4. 6 Protocolos y puertos de la clase de prioridad media

Servicio	Protocolo	Puerto
Directorio Activo	ntp	123
	Kerberos	88
	ldap	389
	microsoft-ds	445
	nbname	137
	nbsession	139
	nbdatagram	138
	RPC, EPM	135
DHCP	UDP	67, 68
DNS	TCP-UDP	53
Symantec Antivirus	TCP	8014
Escritorio Remoto	TCP	3389
	microsoft-ds	445

Carpetas Compartir	nbname	137
	nbsession	139
	nbdatagram	138

4.1.1.1.4 Requerimientos de la Clase de Servicios de Prioridad Baja

En el caso de los servicios con prioridad baja se ha identificado que los requerimientos son mínimos. Los servicios que se utilizan con menos frecuencia pero que pueden ocasionar congestión en algún momento determinado. El ancho de banda mínimo utilizado es de 50 kbps y un máximo de 200 kbps. A continuación se muestran los servicios de prioridad baja identificados.

- SSH
- ICMP
- TELNET
- SNMP
- RELOJ

Por sus requerimientos es importante que sea considerada dentro de la implementación de QoS. Como se muestra la tabla 4.7 de la información recolectada en el capitulo anterior podemos determinar que protocolos y puertos pertenecen dentro de esta clase.

Tabla 4. 7 Protocolos y puertos de la clase de prioridad baja

Servicio	Protocolo	Puerto
Red	SSH	22
	ICMP	N/A
	TELNET	23
	SNMP	161, 162
	TRACEROUTE	N/A
Reloj Biométrico	UDP	4370

4.1.1.1.5 Requerimientos de la Clase por Defecto

En el caso de los servicios que no se entren dentro de ninguna de las categorías mencionadas anteriormente, serán considerados como tráfico por defecto.

4.1.1.2 Marcaje en las clases de tráfico

Con la identificación de las diferentes clases de tráfico y basados en las necesidades de la organización, se definen en las siguientes tablas los valores de marcaje asignados a las diferentes clases de tráfico que se generan dentro de la Unidad de Negocios Termopichincha. El modelo utilizado es DiffServ el cual permite la diferenciación del tráfico basado en la clasificación y marcaje, con el método de marcaje DSCP (Differentiated Service Code Point) en el que está inverso IP Precedence.

Tabla 4. 8 Marcaje Clase de Voz y Video

Clases de Tráfico	Aplicaciones Termopichincha	Valores de Marcaje	
		CAPA 3 DSCP (PHB)	**CAPA 2 CoS**
Clase de Voz y Video	Telefonía IP	46 - (EF) 101110	5
	Videoconferencia	34 - (AF41) 100010	4

En el caso de la clase de voz y video, tabla 4.8, el tráfico debe ser tratado de manera especial, debido a la necesidad de brindar una comunicación clara y sin cortes durante las horas pico, para garantizar un mínimo retardo, perdida de paquetes y ancho de banda garantizado.

En el caso de la Telefonía IP, el marcaje seleccionado es DSCP de tipo EF (PHB) - 46 (DSCP) (101110), debido a que garantiza un retardo mínimo, ancho de banda mínimo, reenvió acelerado y sin probabilidad de descarte. Adicionalmente los 3 primeros bit representan el valor 5 en IP Precedence que identifica prioridad crítica, los 2 bit siguientes representa el valor 11 que indica la máxima probabilidad de NO descarte.

En el caso de la videoconferencia, el marcaje seleccionado es DSCP de tipo AF (PHB) con la clase estándar AF4 - 34 (DSCP) (100010), debido a que garantiza ancho de banda, reenvío seguro y sin probabilidad de descarte. Adicionalmente los 3 primeros bit representan el valor 4 en IP Precedence que identifica prioridad alta, los 2 bit siguientes representa el valor 1 que indica la probabilidad mínima de descarte.

Tabla 4. 9 Marcaje Clase de Servicios de Prioridad Alta

Clases de Tráfico	Aplicaciones Termopichincha	Valores de Marcaje	
		CAPA 3 DSCP (PHB)	**CAPA 2 CoS**
Clase de Servicios de Prioridad Alta	Sistema Financiero IFS	26 - (AF31) 011010	3
	Scada	26 - (AF31) 011010	3
	Aplicaciones Lotus	26 - (AF31) 011010	3
	Correo Electrónico	26 - (AF31) 011010	3
	Base de Datos	26 - (AF31) 011010	3
	Evolution	26 - (AF31) 011010	3

En el caso de la clase de servicios de prioridad alta, tabla 4.9, la necesidad de que las transacciones Financieras, la recolección de datos industriales hacia las entidades públicas reguladoras, solicitudes y flujos de trabajos internos, comunicación y envío de información por correo, transacciones de bases de datos y consultas a los distintos sistemas no sean afectados por la saturación del canal y perdida de paquetes. La indisponibilidad de dichos servicios afectan directamente a los indicadores de gestión del área de TIC, y en peor aún, en el tema industrial ya que las entidades reguladoras pueden emitir sanciones a la organización debido a la indisponibilidad de los datos en línea de generación. En este caso el marcaje seleccionado es DSCP de tipo AF (PHB) con la clase estándar AF3 - 26 (DSCP) (011010), debido a que garantiza: ancho de banda, reenvío seguro y baja probabilidad de descarte. Adicionalmente los 3 primeros bit representan el valor 3 en IP Precedence que identifica prioridad media alta, los 2 bit siguientes representa el valor 1 que indica la probabilidad mínima de descarte.

Tabla 4. 10 Marcaje Clase de Servicios de Prioridad Media

Clases de Tráfico	Aplicaciones Termopichincha	Valores de Marcaje	
		CAPA 3 DSCP (PHB)	**CAPA 2 CoS**
Clase de Servicios de Prioridad Media	Directorio Activo	18 - (AF21) 010010	2
	Asignaciones de direcciones por DHCP	18 - (AF21) 010010	2
	DNS	18 - (AF21) 010010	2
	Symantec Antivirus	18 - (AF21) 010010	2
	Escritorio Remotos	18 - (AF21) 010010	2
	Carpetas Compartidas	18 - (AF21) 010010	2

En el caso de la clase de servicios de prioridad media, tabla 4.10, los servicios de red internos permiten que los usuarios puedan estar vinculados a las diversas aplicaciones. Una sesión correcta al directorio activo, una asignación de dirección ip y la resolución de nombres mediante el DNS son servicios elementales dentro de la infraestructura de red para el consumo de otros servicios. En el caso que los usuarios no tengan estos elementos no podrán cumplir con sus actividades adecuadamente. Adicionalmente se añaden a este grupo tres servicios que son utilizados frecuentemente: carpetas compartidas, accesos remotos y tareas de antivirus. Se ha vuelto muy necesario que las distintas áreas de la organización manejen carpetas compartidas con el objetivo de centralizar la información, disminuir el consumo de recurso de impresión y disponibilidad de la información. En el caso de los accesos remotos, permite manejar servicios centralizados debido a falta de licenciamiento y mejor tiempo de respuesta a los sitios remotos. El monitoreo de los clientes de antivirus mediante una consola centralizada requiere que exista

una sincronización de la información en ambos sentidos y mantener el monitoreo de los eventos que se presenten.

En este caso el marcaje seleccionado es DSCP de tipo AF (PHB) con la clase estándar AF2 - 18 (DSCP) (010010), debido a que garantiza: ancho de banda, reenvío seguro y baja probabilidad de descarte. Adicionalmente los 3 primeros bit representan el valor 2 en IP Precedence que identifica prioridad media, los 2 bit siguientes representa el valor 1 que indica la probabilidad mínima de descarte.

Tabla 4. 11 Marcaje Clase de Servicios de Prioridad Media

Clases de Tráfico	Aplicaciones Termopichincha	Valores de Marcaje	
		CAPA 3 DSCP (PHB)	**CAPA 2 CoS**
Clase de Servicios de Prioridad Baja	SSH, ICMP, TELNET, SNMP, TRACEROUTE	18 - (AF11) 001010	1

En el caso de la clase de servicios de prioridad baja, tabla 4.11, son utilizados con frecuencia por el área de TIC con el objetivo de realizar tareas de administración, monitoreo, pruebas de conectividad, descarga de información, accesos a equipos de comunicación y manejo de configuraciones considerado útil pero no imprescindible.

En este caso el marcaje seleccionado es DSCP de tipo AF (PHB) con la clase estándar AF1 - 10 (DSCP) (001010), debido a que garantiza: reenvío seguro y baja probabilidad de descarte. Adicionalmente los 3 primeros bit representan el valor 1 en IP Precedence que identifica prioridad baja, los 2 bit siguientes representa el valor 1 que indica la probabilidad mínima de descarte.

Por último, en el caso de la clase de servicios por defecto, se asignará el valor de 0 para un comportamiento Best Effort (000000).

4.1.1.3 Mecanismo de encolamiento

Con la identificación de las diferentes clases de tráfico, marcaje seleccionado y basados en las necesidades de la organización, el mecanismo más apropiado para ser aplicado es el CBWFQ, ya que permite la creación de colas para cada clase de tráfico identificado y asignación de ancho de banda según los requerimientos, en este caso, para las clases de Servicios de Prioridad Alta, Servicios de Prioridad Media, Servicios de Prioridad Baja y por Defecto.

En el caso de la Clase de Voz y Video el mecanismo CBWFQ permite dar un tratamiento especial mediante las colas de prioridad estricta, dado que los requerimientos de la voz y video definidas son especialmente para reducir la latencia y mantener un ancho de banda de reserva, LLQ es el mecanismo más apropiado para ser aplicado para este tipo de clase de tráfico.

El ancho de banda que asigna CBWFQ es tomado del máximo valor reservado de una interface que corresponde al 75%, por ello los valores de ancho de banda reservado asignados para cada clase fueron definidos de la siguiente manera:

- Tomando el valor de 4 MB de ancho de banda máximo que se tiene en uno de los enlaces WAN de una de las centrales de Termopichincha y los valores máximos definidos por cada clase, se tiene los siguientes valores:

Tabla 4. 12 Porcentajes de Reserva de cada clase

BW ENLACE	4 MB		
CBWFQ	**Clases de Tráfico**	**Máximo BW por Clases (kbps)**	**Porcentaje Reserva**
75 %	Clase de Voz y Video	800	20
	Clase de Servicios de Prioridad Alta	1600	40
	Clase de Servicios de Prioridad Media	400	10
	Clase de Servicios de Prioridad Baja	200	5
25%	Clase de Servicios por Defecto	1000	25

4.1.1.4 Métodos seleccionados en el diseño

A partir de los métodos seleccionados en el diseño de calidad de servicio, la tabla 4.12 presenta el resumen de cada uno de ellos.

Tabla 4. 13 Métodos seleccionados en el diseño de QoS

PROCESO	MÉTODO
IDENTIFICACIÓN DEL TRÁFICO	NBAR
MODELO	DIFFSERV
CLASIFICACIÓN	PRIORIDAD DEL SERVICO - Clase de Voz y Video - Clase de Servicios de Prioridad Alta - Clase de Servicios de Prioridad Media - Clase de Servicios de Prioridad Baja - Clase por Defecto
MARCAJE	DSCP
CONGESTION	CBWFQ LLQ
CONFIGURACIÓN	MQC (ACL y CLASS MAP)

4.1.2 Implementación de QoS

A partir del método de configuración seleccionado MQC y en base a los resultados del análisis de tráfico, los componentes a definir son:

- Mapa de Clases: Clasificación mediante ALCs.
- Mapa de Políticas: Especifica los parámetros de QoS que se aplican a las clases.
- Política del Servicio: Aplicación del mapa de políticas a una interfaz determinada.

4.1.2.1 Definición de ACLs

Las listas de control de acceso para las distintas clases de tráfico son definidas de la siguiente manera:

- Clase de Voz y Video

ip access-list extended ACL_VOZVIDEO
permit udp any any eq 5060
permit tcp any any eq 5061
permit tcp any any range 1718 1731
permit udp any any range 1718 1731
permit tcp any any eq 5001
permit udp any any eq 5001
permit udp any any range 16384 32767

- Clase de Servicios de Prioridad Alta

ip access-list extended ACL_ALTA
.....IFS......
permit tcp any 172.16.211.0 0.0.0.255 eq 58080
permit tcp any 172.16.211.0 0.0.0.255 eq 59080
permit tcp any 172.16.211.0 0.0.0.255 eq 60080
permit tcp any 172.16.211.0 0.0.0.255 eq 8093

permit tcp any 172.16.212.0 0.0.0.255 eq 58080
permit tcp any 172.16.212.0 0.0.0.255 eq 59080
permit tcp any 172.16.212.0 0.0.0.255 eq 60080
permit tcp any 172.16.212.0 0.0.0.255 eq 8093

permit tcp any 172.16.210.0 0.0.0.255 eq 58080
permit tcp any 172.16.210.0 0.0.0.255 eq 59080
permit tcp any 172.16.210.0 0.0.0.255 eq 60080
permit tcp any 172.16.210.0 0.0.0.255 eq 8093

......SCADA......
permit tcp any any eq 20000
permit tcp any any eq 502
permit tcp any any eq 10001
permit tcp any any eq 4050
permit tcp any any range 7700 7801
permit tcp any any eq 50610
permit tcp any any eq 49333

......LOTUS......
permit tcp any host 192.168.100.3 eq 80
permit tcp any host 192.168.100.3 eq 443
permit tcp any host 192.168.100.3 eq 1352
permit tcp any host 192.168.100.3 eq 1533

permit tcp any host 172.16.128.216 eq 80
permit tcp any host 172.16.128.216 eq 443
permit tcp any host 172.16.128.216 eq 1352

permit tcp any host 172.16.128.164 eq 80
permit tcp any host 172.16.128.164 eq 443
permit tcp any host 172.16.128.164 eq 1352

.....CORREO.....
permit tcp any host 172.16.128.215 eq 1352
permit tcp any host 172.16.128.215 eq 143
permit tcp any host 172.16.128.215 eq 993
permit tcp any host 172.16.128.215 eq 110
permit tcp any host 172.16.128.215 eq 25
permit tcp any host 172.16.128.215 eq 80
permit tcp any host 172.16.128.215 eq 443
permit tcp any host 172.16.128.215 eq 6012

permit tcp any host 172.16.60.21 eq 143
permit tcp any host 172.16. 60.21 eq 993
permit tcp any host 172.16. 60.21 eq 110
permit tcp any host 172.16. 60.21 eq 25
permit tcp any host 172.16. 60.21 eq 80
permit tcp any host 172.16. 60.21 eq 443
permit tcp any host 172.16. 60.21 eq 6012

.....EVOLUTION.....
permit tcp any 172.16.211.0 0.0.0.255 eq 80

.....BASE.DE.DATOS.....
permit tcp any any range 1433 1434
permit tcp any any range 1521 1526

- Clase de Servicios de Prioridad Media

ip access-list extended ACL_MEDIA

.....DNS.....
permit tcp any any eq 53
permit udp any any eq 53

.....DHCP.....
permit udp any any range 67 68

.....ANTIVIRUS.....
permit tcp any any 8014

.....REMOTO.....
permit tcp any any 389

.....CARPETA COMPARTIDA.....
permit udp any any range 137 138
permit tcp any any eq 445

.....AD.....
permit udp any any eq 88
permit tcp any any eq 88
permit udp any any eq 389
permit tcp any any eq 389
permit udp any any eq 123
permit tcp any any eq 123

- Clase de Servicios de Prioridad Baja

ip access-list extended ACL_BAJA
permit udp any any range 161 162
permit tcp any any eq 23
permit icmp any any
permit tcp any any eq 22
permit udp any any 4370

- Clase por Defecto

Todo el tráfico restante

4.1.2.2 Definición de Mapas de Clases y Mapa de Políticas

Los mapas de clases para las distintas clases de tráfico son definidas de la siguiente manera:

- Clase de Voz y Video

class-map match-all VOZVIDEO_IN
match access-group name ***ACL_VOZVIDEO***

class-map match-all VOZVIDEO_OUT
match access-group name ***ACL_VOZVIDEO***

- Clase de Servicios de Prioridad Alta

class-map match-all ALTA_IN
match access-group name ***ACL_ALTA***

class-map match-all ALTA_OUT
match access-group name ***ACL_ALTA***

- Clase de Servicios de Prioridad Media

class-map match-all MEDIA_IN
match access-group name ***ACL_MEDIA***

class-map match-all MEDIA_OUT
match access-group name ***ACL_MEDIA***

- Clase de Servicios de Prioridad Baja

class-map match-all BAJA_IN
match access-group name ***ACL_BAJA***

class-map match-all BAJA_OUT
match access-group name ***ACL_BAJA***

- Clase por Defecto

Los mapas de políticas para las clases antes descritas, tanto para la entrada y salida están definidas de la siguiente manera:

policy-map QOS-IN
class ***VOZVIDEO_IN***
set ip dscp ef
class ***ALTA _IN***
set ip dscp af31
class ***MEDIA _IN***
set ip dscp af21
class ***BAJA _IN***
set ip dscp af11
class ***class-default***
set ip dscp default

policy-map QOS-OUT
class ***VOZVIDEO_OUT***
set ip dscp ef
priority percent 20
class ***ALTA _OUT***
set ip dscp af31
bandwidth percent 40
class ***MEDIA _OUT***
set ip dscp af21
bandwidth percent 10
class ***BAJA _OUT***
set ip dscp af11
bandwidth remaining percent 5
class ***class-default***
fair-queue

4.1.3 Configuración de Equipos de Comunicación

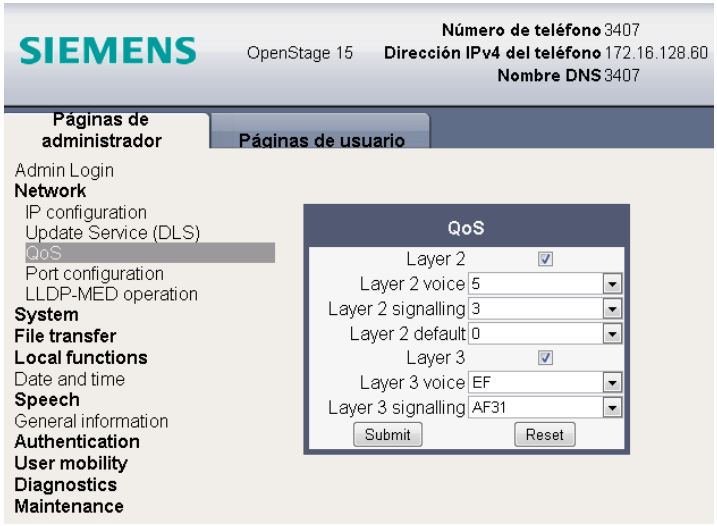
Según lo definido en la implementación de QoS, a continuación se detallan las diferentes configuraciones realizadas tanto en la parte LAN como WAN. Como las configuraciones realizadas para todos los switch y routers, únicamente se detallan las configuraciones de dos equipos.

4.1.3.1 Configuración Teléfonos IP

Una de las recomendaciones al implementar QoS es la definición de la frontera de confianza, en este caso, el primer equipo que se encuentra cerca de la fuente de tráfico son los teléfonos IP de cada usuario.

La figura 4.3 muestra la configuración de QoS aplicada en cada teléfono IP, tanto en capa 2 como en capa 3

Figura 4. 3 Configuración QoS Teléfonos SIEMENS



4.1.3.2 Configuración Switch Cisco

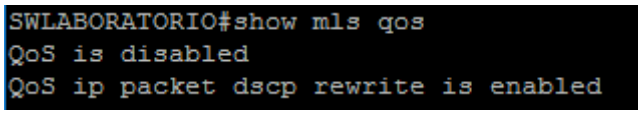
En este caso se tomó como ejemplo la configuración implementada en el switch Catalyst 2960 del área de Laboratorio. Las configuraciones aplicadas están basadas en el documento de Guía de Configuración del software del Switch Catalyst 2960 y 2960s

1. Activación de QoS

   SWLABORATORIO(config)#mls qos
   SWLABORATORIO(config)#no mls qos rewrite ip dscp

   - La figura 4.4 muestra la activación de QoS en los switchs indicados:

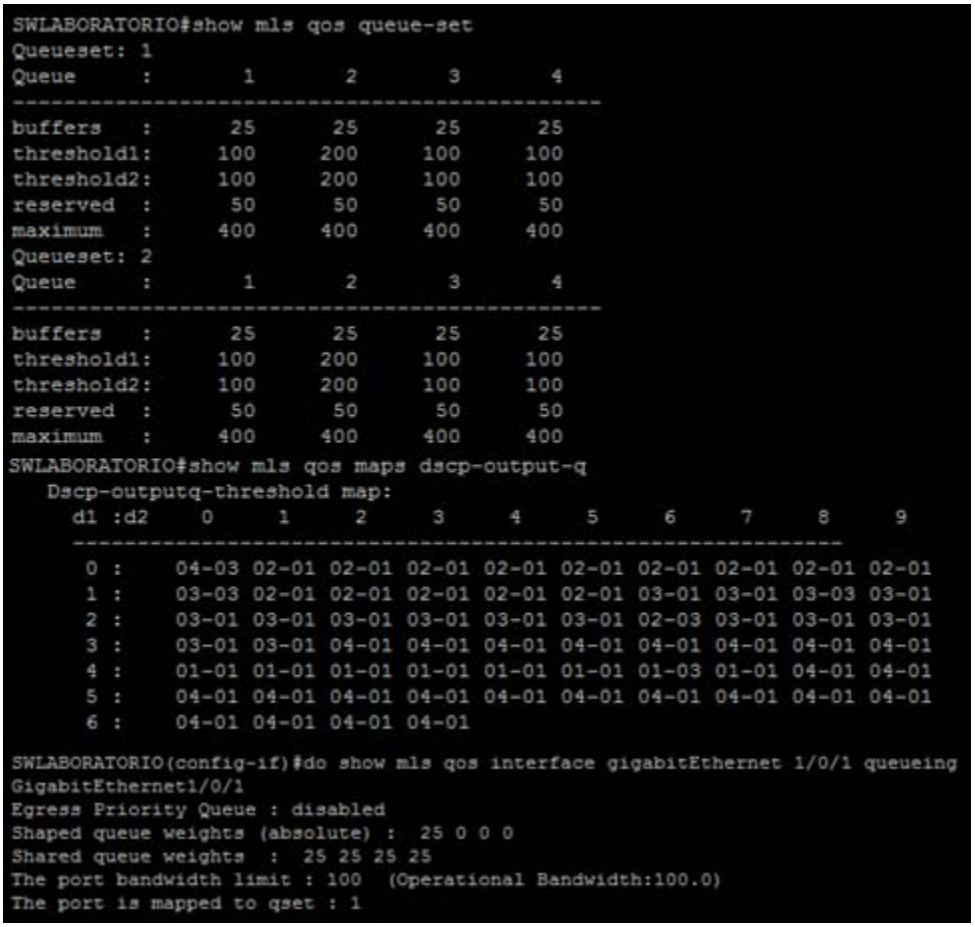
Figura 4. 4 QoS activo Switch Laboratorio



2. A partir de la activación de QoS, se puede realizar el seteo de los parámetros para el tratamiento de los valores de dscp, colas, umbrales, ancho de banda y buffers.

   a) La figura 4.5 muestra los mapas de valores de dscp, colas, umbrales, ancho de banda y buffers seteados por defecto al momento de habilitar QoS. Es importante saber que los modelos Catalyst 2960s no soportan las configuraciones de colas de entrada, por ello, únicamente se trabajará con las colas de salida. Como se puede observa se trabaja con 4 colas de salida con 3 umbrales.

Figura 4. 5 Parámetros Iniciales QoS



```
SWLABORATORIO#show mls qos queue-set
Queueset: 1
Queue     :       1       2       3       4
----------------------------------------------
buffers   :      25      25      25      25
threshold1:     100     200     100     100
threshold2:     100     200     100     100
reserved  :      50      50      50      50
maximum   :     400     400     400     400
Queueset: 2
Queue     :       1       2       3       4
----------------------------------------------
buffers   :      25      25      25      25
threshold1:     100     200     100     100
threshold2:     100     200     100     100
reserved  :      50      50      50      50
maximum   :     400     400     400     400
SWLABORATORIO#show mls qos maps dscp-output-q
   Dscp-outputq-threshold map:
     d1 :d2    0     1     2     3     4     5     6     7     8     9
     ------------------------------------------------------------
      0 :    04-03 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01
      1 :    03-03 02-01 02-01 02-01 02-01 02-01 03-01 03-01 03-03 03-01
      2 :    03-01 03-01 03-01 03-01 03-01 03-01 02-03 03-01 03-01 03-01
      3 :    03-01 03-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
      4 :    01-01 01-01 01-01 01-01 01-01 01-01 01-03 01-01 04-01 04-01
      5 :    04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
      6 :    04-01 04-01 04-01 04-01

SWLABORATORIO(config-if)#do show mls qos interface gigabitEthernet 1/0/1 queueing
GigabitEthernet1/0/1
Egress Priority Queue : disabled
Shaped queue weights (absolute) :  25 0 0 0
Shared queue weights  :  25 25 25 25
The port bandwidth limit : 100  (Operational Bandwidth:100.0)
The port is mapped to qset : 1
```

b) Tomando en cuenta los valores asignados en el marcaje (DSCP), la tabla 4.13 muestra los valores asignados a las diferentes clases para el tratamiento de las colas, umbrales y buffer.

Tabla 4. 14 Valores DSCP, Colas, Umbral, Buffer y Ancho de Banda

CLASES	VALORES DSCP	COLAS	UMBRAL	BUFFER	AB
Clase de Voz y Video	dscp ef (46) cos 5	1	3	40	40
Clase de Servicios de Prioridad Alta	dscp af31 (26) cos 3	2	3	30	30
Clase de Servicios de Prioridad Media	dscp af21 (18) cos 2	3	3	20	20
Clase de Servicios de Prioridad Baja	dscp af11 (10) cos 1	3	3		
Clase por Defecto	dscp default (0) cos 0	4 4	3 2	10	10

c) Con el siguiente comando se realiza la asignación de los valores dscp y cos a las colas con los umbrales según cuadro de valores.

SWLABORATORIO(config)#mls qos srr-queue output dscp-map queue 1 threshold 3 46
SWLABORATORIO(config)#mls qos srr-queue output dscp-map queue 2 threshold 3 26
SWLABORATORIO(config)#mls qos srr-queue output dscp-map queue 3 threshold 3 18 10
SWLABORATORIO(config)#mls qos srr-queue output dscp-map queue 4 threshold 1 0

SWLABORATORIO(config)#mls qos srr-queue output cos-map queue 1 threshold 3 5
SWLABORATORIO(config)#mls qos srr-queue output cos-map queue 2 threshold 3 3
SWLABORATORIO(config)#mls qos srr-queue output cos-map queue 3 threshold 3 2
SWLABORATORIO(config)#mls qos srr-queue output cos-map queue 4 threshold 2 0
SWLABORATORIO(config)#mls qos srr-queue output cos-map queue 4 threshold 3 1

d) Con el siguiente comando se realiza la asignación de los buffers de las colas según cuadro de valores.

SWLABORATORIO(config)#mls qos queue-set output 1 buffers 40 30 20 10

e) Como se puede identificar en la tabla 4.13, la cola 1 tiene asignado el tráfico de la clase de voz y video, por ello, se debe atender como prioritaria y vaciarse antes de comenzar con las siguientes colas. El siguiente comando permite asignar como prioridad a la cola 1 dentro de cada una de las interfaces.

SWLABORATORIO(config)#interface gigabitEthernet 1/0/1
SWLABORATORIO(config-if-range)#queue-set 1
SWLABORATORIO(config-if-range)#priority-queue out

f) Con el siguiente comando se realiza la asignación del ancho de banda compartido para las diferentes colas.

SWLABORATORIO(config)#interface gigabitEthernet 1/0/1
SWLABORATORIO(config-if-range)#srr-queue bandwidth share 1 45 35 20

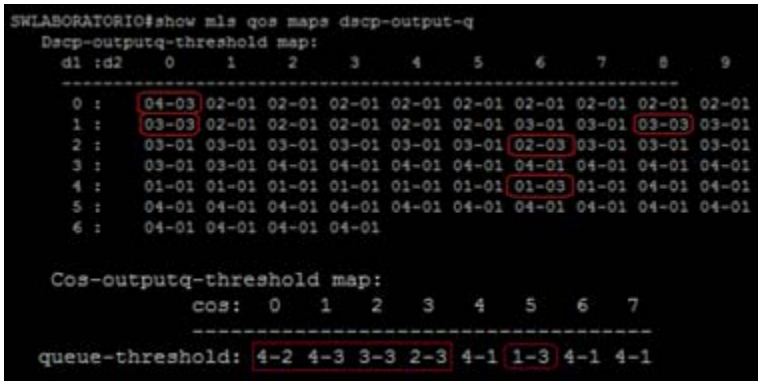
g) Con el siguiente comando se indica a las diferentes interfaces que confíen en los valores de cos.

SWLABORATORIO(config)#interface gigabitethernet1/0/1
SWLABORATORIO(config-int)#mls qos trust cos

3. Verificación de los valores parametrizados de dscp, cos, colas, umbrales, ancho de banda y buffers.

a) La figura 4.6 muestra el mapa de valores dscp y cos asignados a las colas y umbrales de salida. La tabla de mapa de dscp-cos se utiliza para calcular el valor de CoS si el puerto está configurado para confianza DSCP. Del mismo modo, la tabla de mapa de cos-dscp se utiliza para calcular el valor DSCP si el puerto es configurado para confiar en CoS.

Figura 4. 6 Mapa de Valores DSCP y CoS



b) La figura 4.7 muestra los valores de los buffers asignados a las colas.

Figura 4. 7 Valores de Colas

```
SWLABORATORIO#show mls qos queue-set
Queueset: 1
Queue     :       1       2       3       4
----------------------------------------------
buffers   :      40      30      20      10
threshold1:     100     200     100     100
threshold2:     100     200     100     100
reserved  :      50      50      50      50
maximum   :     400     400     400     400
Queueset: 2
Queue     :       1       2       3       4
----------------------------------------------
buffers   :      25      25      25      25
threshold1:     100     200     100     100
threshold2:     100     200     100     100
reserved  :      50      50      50      50
maximum   :     400     400     400     400
```

c) La figura 4.8 muestra los valores de los anchos de bandas compartidos asignados a cada interfaz.

Figura 4. 8 Valores compartidos de ancho de banda de la interfaz

```
SWLABORATORIO(config-if)#do show mls qos interface gigabitEthernet 1/0/1 queueing
GigabitEthernet1/0/1
Egress Priority Queue : enabled
Shaped queue weights (absolute) :  25 0 0 0
Shared queue weights  :  1 45 35 20
The port bandwidth limit : 100  (Operational Bandwidth:100.0)
The port is mapped to qset : 1
```

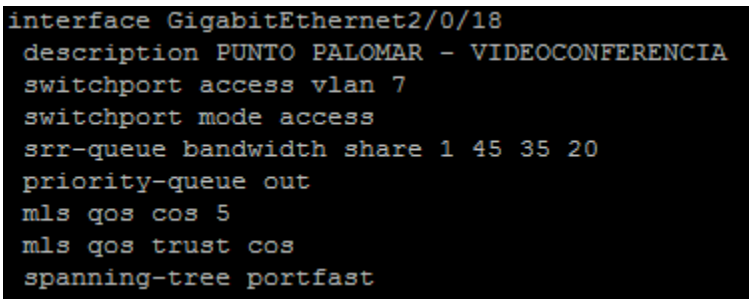
d) La figura 4.9 muestra los parámetros configurados en las interfaces.

Figura 4. 9 Parámetros QoS interfaz

```
interface GigabitEthernet1/0/25
 description TRUNK UPLINK DATACENTER
 switchport mode trunk
 srr-queue bandwidth share 1 45 35 20
 priority-queue out
 mls qos trust cos
```

e) La figura 4.10 muestra los parámetros configurados en el SWDATACENTER, específicamente en la interfaz donde se encuentra conectado el equipo de videoconferencia Polycom, asignando un valor constante de CoS de 5.

Figura 4. 10 Parámetros QoS interfaz videoconferencia SWDATACENTER



4.1.3.3 Configuración Router Cisco

En este caso se tomó como ejemplo la configuración implementada en el router Cisco 1921 del área del Data Center - Guangopolo con la Clase de Voz y Video de mayor prioridad.

1. Creación de la lista de control de acceso extendida, mediante el siguiente comando:

ROUTERGPO#conf ter
ROUTERGPO(config)#ip access-list extended ACL_VOZVIDEO
ROUTERGPO(config-ext-nacl)#permit udp any any eq 5060
ROUTERGPO(config-ext-nacl)#permit tcp any any eq 5061
ROUTERGPO(config-ext-nacl)#permit tcp any any range 1718 1731
ROUTERGPO(config-ext-nacl)#permit udp any any range 1718 1731
ROUTERGPO(config-ext-nacl)#permit tcp any any eq 5001
ROUTERGPO(config-ext-nacl)#permit udp any any eq 5001
ROUTERGPO(config-ext-nacl)#permit udp any any range 16384 32767

a) La figura 4.11 muestra la lista de control de acceso de la Clases de Voz y Video creada y los matchs que se realizan de cada acceso.

Figura 4. 11 ACL de la Clase de Voz y Video ROUTERGPO

```
ROUTERGPO#show access-lists
Extended IP access list ACL_VOZVIDEO
    10 permit udp any any eq 5060 (7268 matches)
    20 permit tcp any any eq 5061
    30 permit tcp any any range 1718 1731 (10821 matches)
    40 permit udp any any range 1718 1731 (1713 matches)
    50 permit tcp any any eq 5001
    60 permit udp any any eq 5001
    70 permit udp any any range 16384 32767 (109942 matches)
```

2. Creación del mapa de la clase relacionada con las lista de control de acceso ACL-VOZVIDEO mediante el siguiente comando:

ROUTERGPO#conf ter
ROUTERGPO(config)#class-map match-all VOZVIDEO_OUT
ROUTERGPO(config-cmap)#match access-group name ACL_VOZVIDEO
ROUTERGPO(config-cmap)#exit
ROUTERGPO(config)#class-map match-all VOZVIDEO_IN
ROUTERGPO(config-cmap)#match access-group name ACL_VOZVIDEO
ROUTERGPO(config-cmap)#exit

a) La figura 4.12 muestra el mapa de clase creado y relacionado a la lista de control de acceso ACL_VOZVIDEO.

Figura 4. 12 Class Map de la Clase de Voz y Video ROUTERGPO

```
ROUTERGPO#show class-map
 Class Map match-all VOZVIDEO_OUT (id 2)
   Match access-group name ACL_VOZVIDEO
 Class Map match-all VOZVIDEO_IN (id 1)
   Match access-group name ACL_VOZVIDEO
```

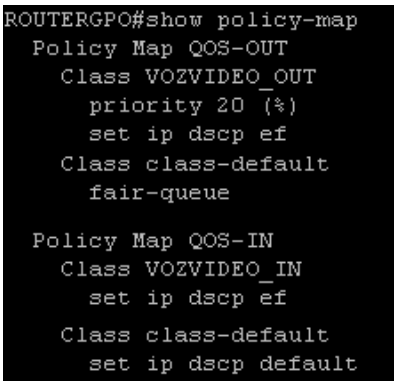
3. Creación de las políticas de entrada IN y de salida OUT relacionada con el mapa de la clase, mediante el siguiente comando:

ROUTERGPO(config)#policy-map QOS-OUT
ROUTERGPO(config-pmap)#class VOZVIDEO_OUT
ROUTERGPO(config-pmap-c)#priority percent 30
ROUTERGPO(config-pmap-c)#set ip dscp ef
ROUTERGPO(config)#exit

ROUTERGPO(config)#policy-map QOS-IN
ROUTERGPO(config-pmap)#class VOZVIDEO_IN
ROUTERGPO(config-pmap-c)#set ip dscp ef
ROUTERGPO(config)#exit

a) La figura 4.13 muestra las políticas creadas y relacionadas con los mapas de las clases.

Figura 4. 13 Policy Map IN y OUT ROUTERGPO

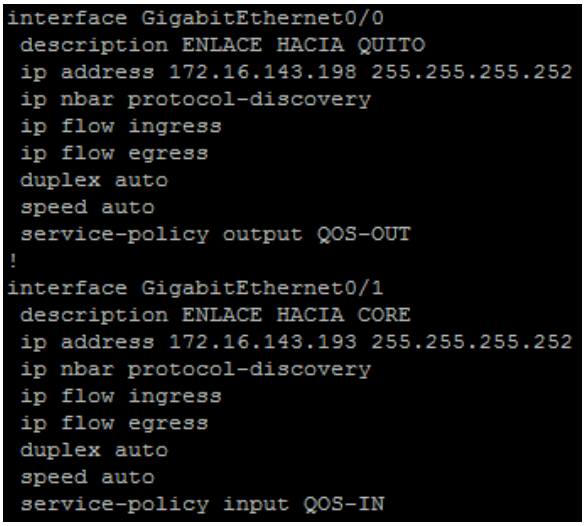


4. Asignación de las políticas en las interfaces de entrada y salida, mediante el siguiente comando:

ROUTERGPO#conf ter
ROUTERGPO(config)#interface gigabitEthernet 0/1
ROUTERGPO(config-if)#service-policy input QOS-IN
ROUTERGPO(config)#interface gigabitEthernet 0/0
ROUTERGPO(config-if)#service-policy output QOS-OUT

a) La figura 4.14 muestra la política asignada a las interfaces según las necesidades de entrada IN y salida OUT.

Figura 4. 14 Service-Policy interfaces ROUTERGPO



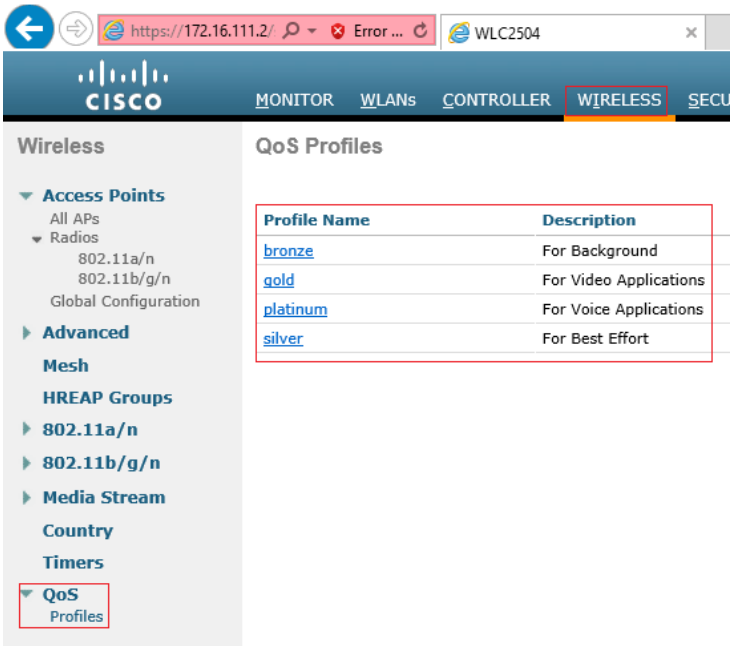
4.1.3.4 Configuración Wireless Cisco

En este caso se tomó como ejemplo la configuración que presenta por defecto en la controladora LAN de la red Wireless. Esta controladora soporta 4 niveles de Qos:

- Platinum/Voice que soporta una alta calidad de servicio para voz sobre redes inalámbricas.
- Gold/Video que soporta alta calidad de servicio para aplicaciones de video.
- Bronze/Background que soporta un menor ancho de banda para redes de invitados.
- Silver/Best Effort que soporta ancho de banda normal para los clientes siendo la configuración por defecto presentada en el equipo.

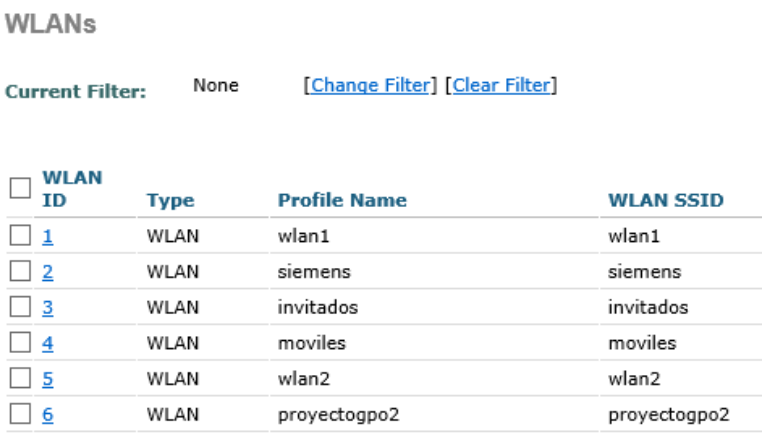
La figura 4.15 muestra los perfiles creados QoS según los 4 niveles soportados.

Figura 4. 15 Perfiles QoS - WLC



Las diferentes wlans que se manejan dentro de la red interna poseen asignado un perfil especifico de QoS, la cual está relacionada con el propósito de cada uno de las wlas. La siguiente figura 4.16 muestra las redes wlan que se manejan actualmente:

Figura 4. 16 Redes WLAN Termopichincha



La red wlan SIEMENS es una red creada para la utilización de teléfonos wireless SIEMENS, esta red pertenece a una VLAN dedicada a telefonía, por ello, fue asignado el perfil de *Platinum*. La red wlan INVITADOS es una red creada para la utilización de usuarios externos, por ello, fue asignado el perfil de *Bronce*. Las redes wlan WLAN1, MOVILES, WLAN2 y PROYECTOSGPO2 son redes utilizadas por usuarios internos que tienen asignado un equipo portátil de la organización, por ello, fue asignado el perfil de Silver. La figura 4.17 muestra las configuraciones aplicadas.

Figura 4. 17 QoS aplicadas en WLAN Termopichincha

4.1.4 Resultados

4.1.4.1 Comprobación de Resultados

Las siguientes imágenes muestran los valores estadísticos obtenidos, a partir de la aplicación de QoS dentro de los equipos de comunicación.

En el caso del SWLABORATORIO, a partir de las configuraciones realizadas, se puede identificar que el tráfico se encuentra clasificado según los parámetros asignados a las colas y umbrales de salida. En el caso de la clase de Voz y Video el parámetro de dscp es 46 - cola 1

umbral 3, en la clase de prioridad ALTA el parámetro de dscp es 26 - cola 2 umbral 3, en la clase de prioridad MEDIA el parámetro de dscp es 18 - cola 3 umbral 3, en la clase de prioridad BAJA el parámetro de dscp es 18 - cola 3 umbral 3 y el tráfico restante con el parámetro dscp 0 - cola 4 umbral 1. La figura 4.18 muestra la salida dscp, la figura 4.19 muestra la salida cos y la figura 4.20 muestra el tráfico de las colas y umbrales de la interface gigabitEthernet 1/0/25 de tipo trunk.

Figura 4. 18 Salida dscp interface gigabitEthernet 1/0/25

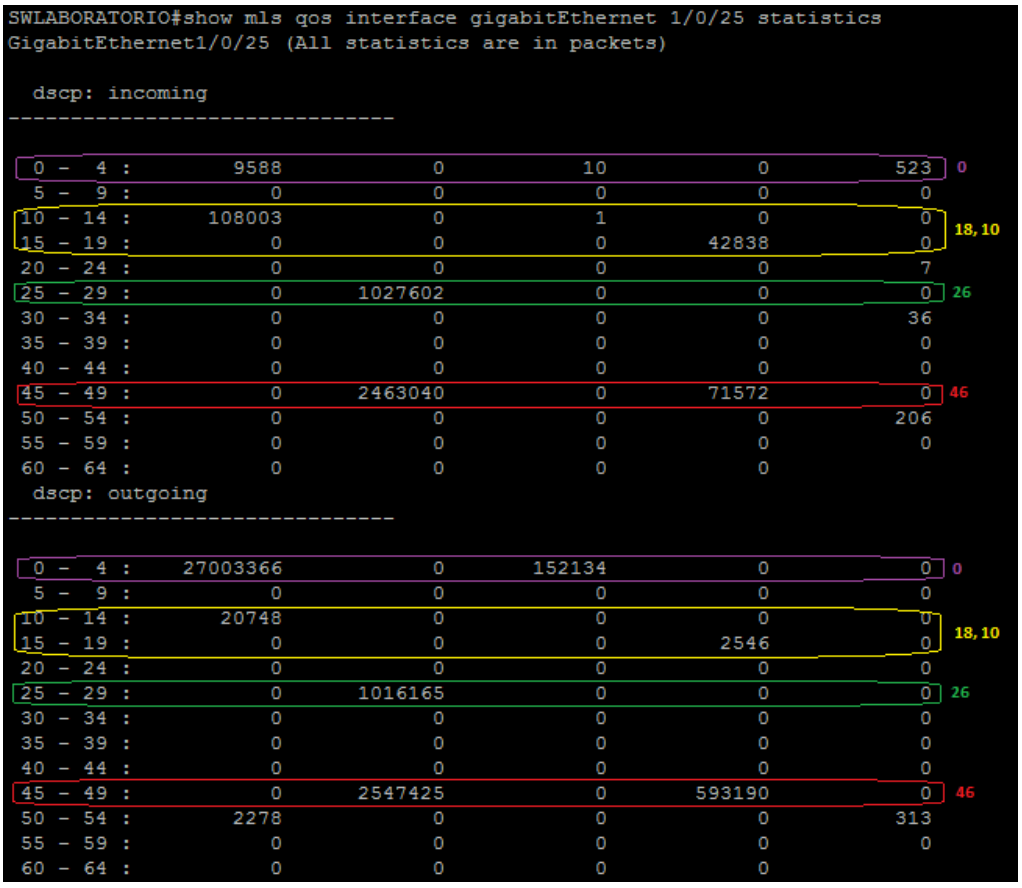
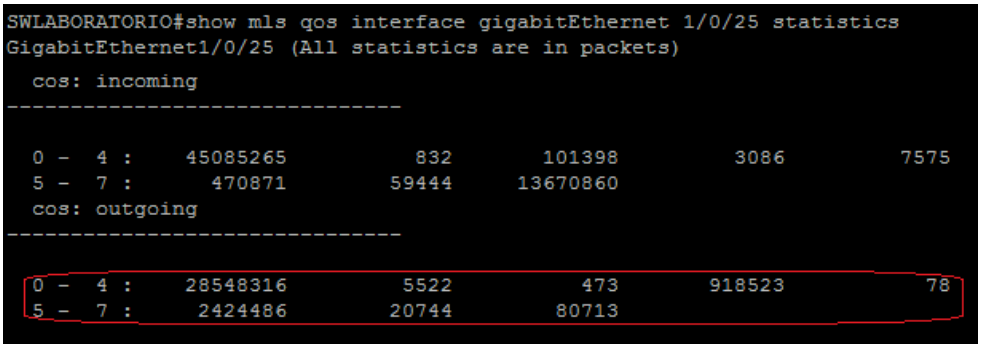
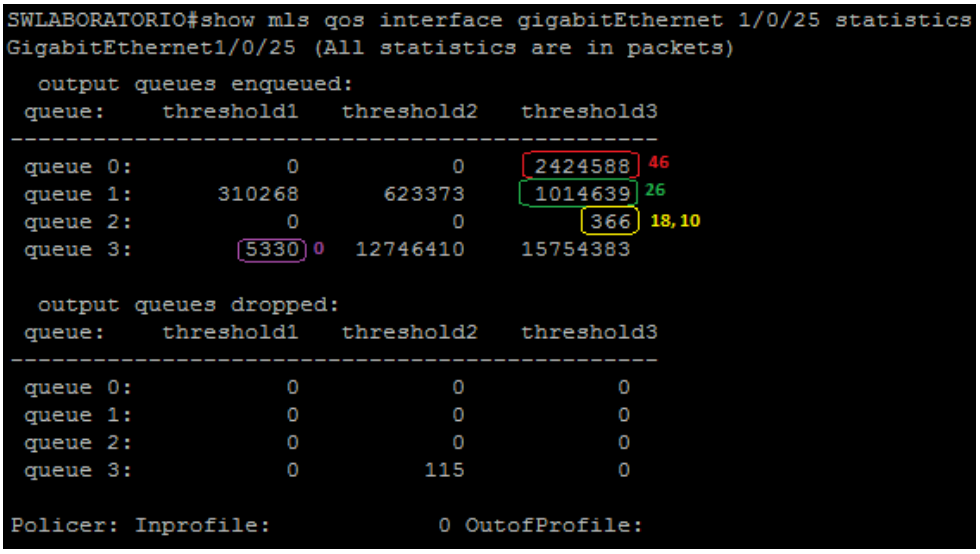


Figura 4. 19 Salida cos interface gigabitEthernet 1/0/25



```
SWLABORATORIO#show mls qos interface gigabitEthernet 1/0/25 statistics
GigabitEthernet1/0/25 (All statistics are in packets)
  cos: incoming
-------------------------------

  0 -  4 :    45085265          832       101398         3086         7575
  5 -  7 :      470871        59444     13670860
  cos: outgoing
-------------------------------

  0 -  4 :    28548316         5522          473       918523           78
  5 -  7 :     2424486        20744        80713
```

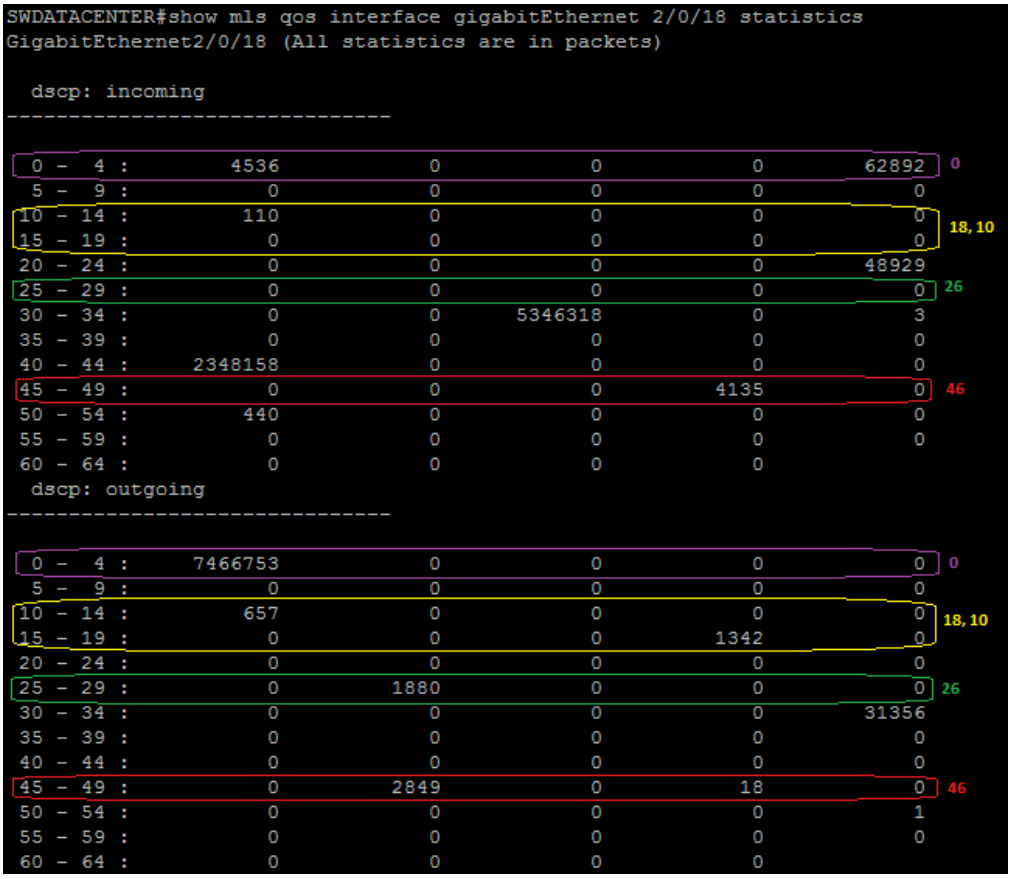
Figura 4. 20 Colas y Umbrales de la interface gigabitEthernet 1/0/25



```
SWLABORATORIO#show mls qos interface gigabitEthernet 1/0/25 statistics
GigabitEthernet1/0/25 (All statistics are in packets)
  output queues enqueued:
 queue:    threshold1   threshold2   threshold3
-----------------------------------------------
 queue 0:           0            0      2424588 46
 queue 1:      310268       623373      1014639 26
 queue 2:           0            0          366 18, 10
 queue 3:        5330 0   12746410     15754383

  output queues dropped:
 queue:    threshold1   threshold2   threshold3
-----------------------------------------------
 queue 0:           0            0            0
 queue 1:           0            0            0
 queue 2:           0            0            0
 queue 3:           0          115            0

Policer: Inprofile:            0 OutofProfile:
```

En el caso del SWDATACENTER, en la figura 4.21 se muestran los siguientes resultados aplicados a la interfaz que mantiene conexión directa al equipo de videoconferencia Polycom de Guangopolo.

Figura 4. 21 Salida dscp interface gigabitEthernet 2/0/18



En el caso del ROUTERGPO, a partir de las configuraciones realizadas, se puede identificar que el tráfico se encuentra clasificado y marcado según los parámetros asignados. La figura 4.22 muestra el número de paquetes marcados y la figura 4.23 muestra la clasificación realizada mediante la lista de control de acceso, ambas relacionadas a la Clase de Voz y Video.

Figura 4. 22 Marcaje de paquetes ROUTERGPO QOS - IN y QOS-OUT

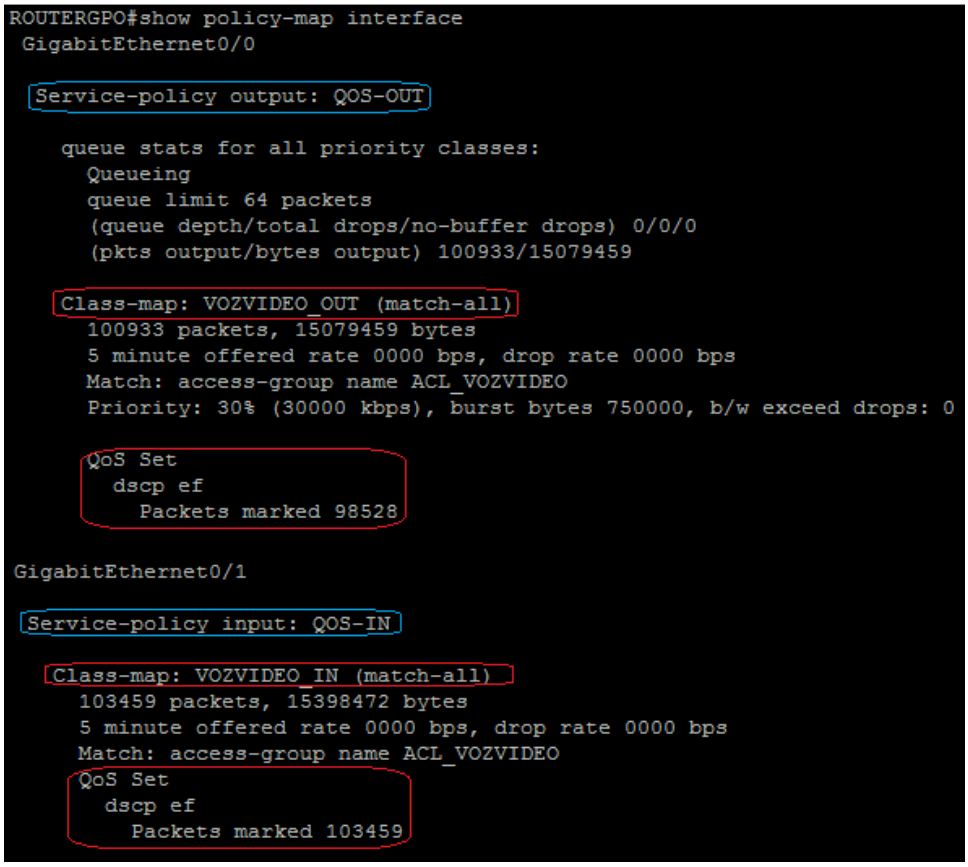
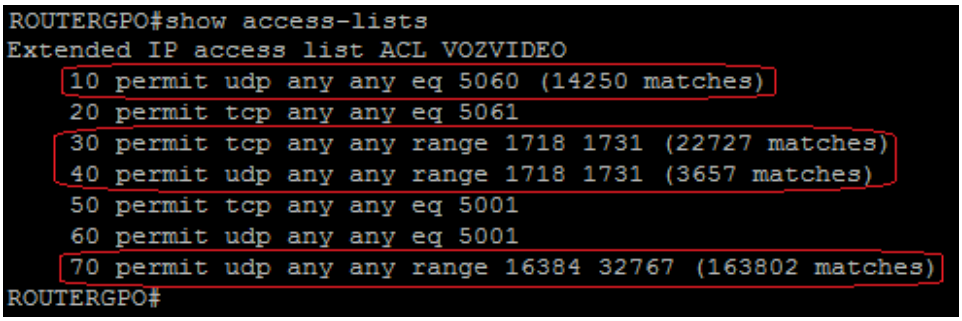


Figura 4. 23 Clasificación de paquetes ROUTERGPO - ACL



En el caso de los equipos routers ubicadas en las centrales remotas Quevedo (ROUTERQUEVEDO) y Jivino (ROUTERJIVINO), las siguientes figuras 4.24 y 4.25 muestran el resultado obtenido.

Figura 4. 24 Marcaje de paquetes ROUTERJIVINO QOS - IN y QOS-OUT

```
ROUTERJIVINO#show policy-map interface
 FastEthernet4

  Service-policy output: QOS-OUT

    queue stats for all priority classes:
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 14175/2904379

    Class-map: VOZVIDEO_OUT (match-all)
      14175 packets, 2904379 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name ACL_VOZVIDEO
      Priority: 30% (30000 kbps), burst bytes 750000, b/w exceed drops: 0

      QoS Set
        dscp ef
          Packets marked 14175

Vlan2

  Service-policy input: QOS-IN

    Class-map: VOZVIDEO_IN (match-all)
      15675 packets, 3183175 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name ACL_VOZVIDEO
      QoS Set
        dscp ef
          Packets marked 15675
```

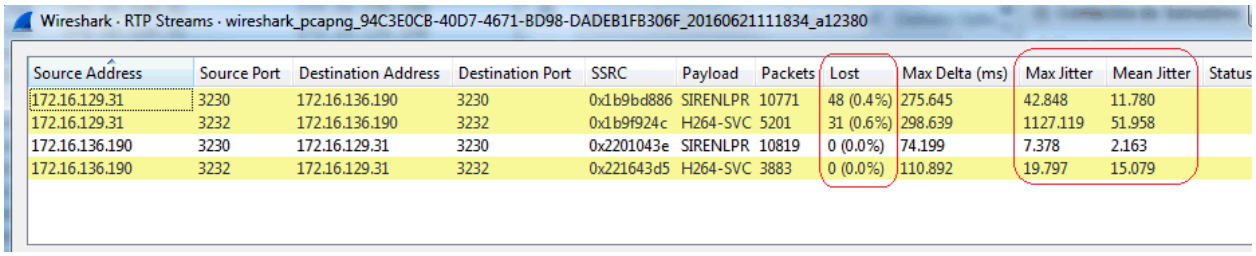
Figura 4. 25 Marcaje de paquetes ROUTERQUEVEDO QOS - IN y QOS-OUT

```
ROUTERQUEVEDO#show policy-map interface
 FastEthernet4

  Service-policy output: QOS-OUT

    queue stats for all priority classes:
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 198549/38319139

    Class-map: VOZVIDEO_OUT (match-all)
      198549 packets, 38319139 bytes
      5 minute offered rate 25000 bps, drop rate 0000 bps
      Match: access-group name ACL_VOZVIDEO
      Priority: 30% (30000 kbps), burst bytes 750000, b/w exceed drops: 0

      QoS Set
        dscp ef
          Packets marked 196431

Vlan2

  Service-policy input: QOS-IN

    Class-map: VOZVIDEO_IN (match-all)
      192973 packets, 37984899 bytes
      5 minute offered rate 25000 bps, drop rate 0000 bps
      Match: access-group name ACL_VOZVIDEO
      Match: protocol rtp audio
      QoS Set
        dscp ef
          Packets marked 192973
```

De las pruebas realizadas durante la hora pico y las horas de mayor tráfico, se tiene el siguiente comportamiento al momento de establecer una videoconferencia y una llamada hacia un sitio remoto.

La figura 4.26 muestra los valores de pérdida de paquetes y jitter al establecer una llamada de videoconferencia hacia la Central Quevedo. Adicionalmente la figura 4.27 muestra la imagen de la videoconferencia establecida durante la misma prueba.

Figura 4. 26 Valores de Lost y Jitter videoconferencia Quevedo

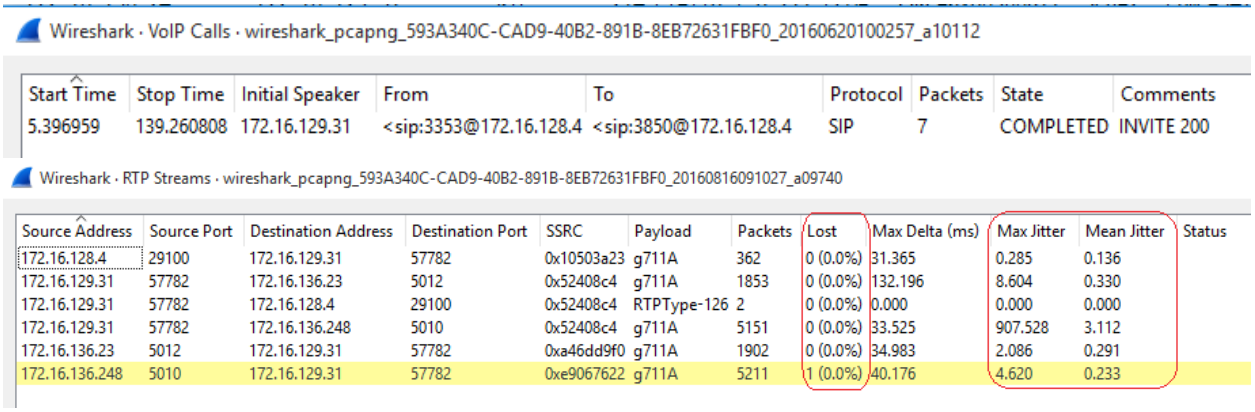


Source Address	Source Port	Destination Address	Destination Port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
172.16.129.31	3230	172.16.136.190	3230	0x1b9bd886	SIRENLPR	10771	48 (0.4%)	275.645	42.848	11.780	
172.16.129.31	3232	172.16.136.190	3232	0x1b9f924c	H264-SVC	5201	31 (0.6%)	298.639	1127.119	51.958	
172.16.136.190	3230	172.16.129.31	3230	0x2201043e	SIRENLPR	10819	0 (0.0%)	74.199	7.378	2.163	
172.16.136.190	3232	172.16.129.31	3232	0x221643d5	H264-SVC	3883	0 (0.0%)	110.892	19.797	15.079	

Figura 4. 27 Videoconferencia Quevedo sin QoS

La figura 4.28 muestra los valores de pérdida de paquetes y jitter al establecer una llamada telefónica mediante la aplicación de X-lite con una cuenta SIP configurada.

Figura 4. 28 Valores de lost y jitter llamada telefónica Quevedo



Wireshark · VoIP Calls · wireshark_pcapng_593A340C-CAD9-40B2-891B-8EB72631FBF0_20160620100257_a10112

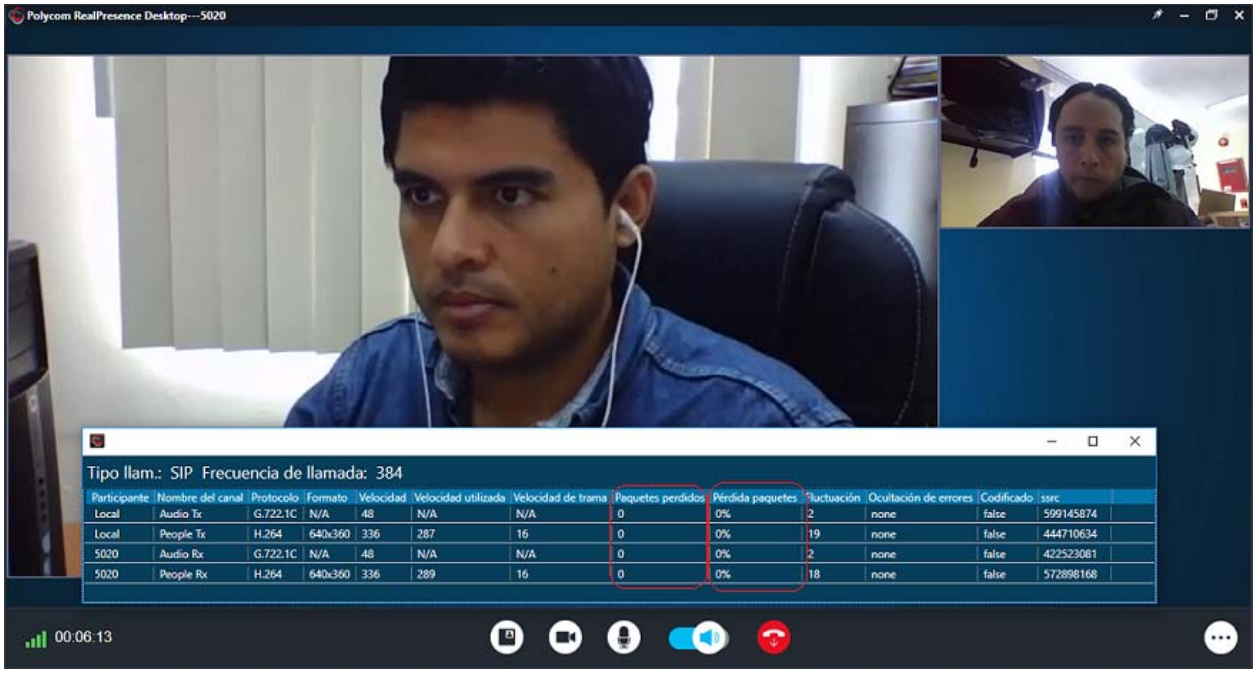
Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
5.396959	139.260808	172.16.129.31	<sip:3353@172.16.128.4	<sip:3850@172.16.128.4	SIP	7	COMPLETED	INVITE 200

Wireshark · RTP Streams · wireshark_pcapng_593A340C-CAD9-40B2-891B-8EB72631FBF0_20160816091027_a09740

Source Address	Source Port	Destination Address	Destination Port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
172.16.128.4	29100	172.16.129.31	57782	0x10503a23	g711A	362	0 (0.0%)	31.365	0.285	0.136	
172.16.129.31	57782	172.16.136.23	5012	0x52408c4	g711A	1853	0 (0.0%)	132.196	8.604	0.330	
172.16.129.31	57782	172.16.128.4	29100	0x52408c4	RTPType-126	2	0 (0.0%)	0.000	0.000	0.000	
172.16.129.31	57782	172.16.136.248	5010	0x52408c4	g711A	5151	0 (0.0%)	33.525	907.528	3.112	
172.16.136.23	5012	172.16.129.31	57782	0xa46dd9f0	g711A	1902	0 (0.0%)	34.983	2.086	0.291	
172.16.136.248	5010	172.16.129.31	57782	0xe9067622	g711A	5211	1 (0.0%)	40.176	4.620	0.233	

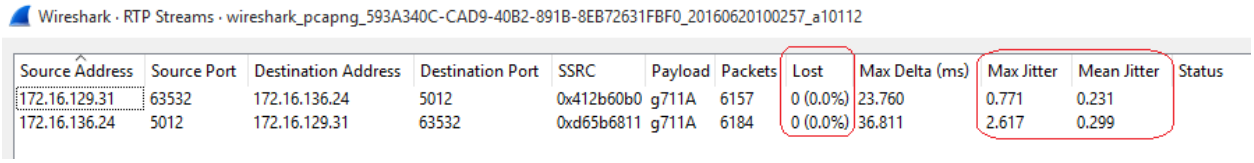
Con la aplicación de las políticas de QoS, se puede evidenciar la diferencia al momento de establecer una videoconferencia y una llamada hacia el sitio remoto. La figura 4.29 muestra los valores de pérdida de paquetes en 0% y la imagen presenta una mayor nitidez.

Figura 4. 29 Videoconferencia Quevedo con QoS



La figura 4.30 muestra la reducción de los valores al momento de establecer la misma llamada telefónica mediante la aplicación X-Lite

Figura 4. 30 Llamada telefónica Quevedo con QoS


Wireshark · RTP Streams · wireshark_pcapng_593A340C-CAD9-40B2-891B-8EB72631FBF0_20160620100257_a10112

Source Address	Source Port	Destination Address	Destination Port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
172.16.129.31	63532	172.16.136.24	5012	0x412b60b0	g711A	6157	0 (0.0%)	23.760	0.771	0.231	
172.16.136.24	5012	172.16.129.31	63532	0xd65b6811	g711A	6184	0 (0.0%)	36.811	2.617	0.299	

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Al realizar el análisis de la infraestructura de red física de la Unidad de Negocios Termopichincha se evidenció que en la ubicación de la Central Térmica Guangopolo existen actualmente 7 nodos ubicados en diferentes áreas e interconectados mediante canales de fibra óptica que convergen dentro del Data Center, dicho canal de fibra óptica es de tipo multimodo y monomodo, lo cual complica la interconexión de otros sitios utilizando estos mismos canales. Al tener fibra óptica de diferentes tipos provoca que el área de TIC realice la adquisición de diferentes tipos de equipamiento y aplicar otras métodos de conexión, generando puntos de fallas importantes dentro de la infraestructura de red física de la Unidad de Negocios Termopichincha
- Al realizar el análisis de la infraestructura de red física de la Unidad de Negocios Termopichincha se evidenció un punto de falla que causaría una indisponibilidad de todos los servicios y especialmente afectaría a la comunicación hacia la matriz de CELEC. El canal de comunicación entre las Oficinas de Quito y la Central Térmica de Guangopolo es mediante un canal de fibra óptica de aproximadamente 30 kilómetros, en el momento de que exista una falla física en el canal o una falla en el equipamiento de comunicaciones, el canal dejaría de funcionar provocando la indisponibilidad de los servicios, generando un problema crítico que afectaría a toda la Unidad de Negocios Termopichincha.

- Al realizar el análisis del servicio de telefonía IP, se pudo obtener datos muy precisos y constantes debido a que la central telefónica maneja un número máximo de usuarios sin oportunidad de crecimiento y los controles de utilización de la telefonía son muy estrictos y restringidos. Su falencia está en su limitante de crecimiento, provocando que la QoS implementada para este servicio solo sea aprovechada por los usuarios que manejan una extensión IP. Igualmente con el servicio de videoconferencia, se tienen datos constantes y precisos debido a que la administración y utilización del servicio es manejada por el departamento de TIC evitando que los usuarios manipulen el servicio a su conveniencia.
- Durante el análisis realizado a los equipos de comunicación (switch, routers, access point, etc) se pudo evidenciar que estos poseen las características necesarias y suficientes para poder soportar configuraciones de QoS, provocando que la Unidad de Negocios Termopichincha no necesite realizar la renovación de equipamiento de comunicaciones durante los próximos 4 a 5 años, obviamente tomando en cuenta que el factor de crecimiento de usuarios y servicios de red es limitada. Los equipos de comunicación mantienen sus garantías de soporte vigentes y se encuentran en constante seguimiento por parte del área de TIC mediante las herramientas de monitoreo. Por otro lado, hablando del tema financiero y evaluando la última compra realizada en renovación de equipos de comunicación, la Unidad de Negocios realizó una inversión de aproximadamente $30.000 dólares. Realizando una proyección de 4 a 5 años en que los equipos actuales continuarían con su funcionamiento normal, se ahorraría una cantidad de $150.000 dólares representando un valor significativo para

el Plan Operativo Anual del área de TIC que puede ser invertido en el mejoramiento de otros servicios.

- Durante el trabajo realizado con el área de TIC en la identificación y clasificación del tráfico de la red, se pudo definir los requerimientos necesarios y prioritarios para los servicios transaccionales, documentales, industriales y de comunicaciones, agrupándolos en 5 clases de tráfico: Clase de Voz y Video, Clase de Servicios de Prioridad Alta, Clase de Servicios de Prioridad Media, Clase de Servicios de Prioridad Baja y Clase por Defecto. Cada una de las clases posee aplicaciones específicas que son utilizadas diariamente por los usuarios para el cumplimiento de sus actividades, como también, contiene aplicaciones que son utilizadas y controladas por entidades de control externas.
- Para la implementación de QoS se seleccionó como método principal de identificación de tráfico a NBAR debido a que los equipos mantienen un estándar en cuanto a su marca (Cisco); se seleccionó el modelo de implementación DiffServ por su gran escalabilidad y diferenciación del tráfico en clases ofreciendo varios niveles de servicios; se seleccionó el tipo de marcaje mediante el valor de DSCP por su composición de 6 bits ofreciendo mayor nivel de servicios; se seleccionó el método de encolamiento CBWFQ y LLQ que ofrecen mecanismos avanzados para la asignación de ancho de banda, clasificación del tráfico y tratamiento prioritario para el tráfico de tiempo real; y por último se seleccionó el método de configuración MQC (ACL y CLASS MAP) ya que es muy recomendado para realizar configuraciones manuale en los equipos de comunicación.

- A partir de la aplicación de las políticas de QoS dentro de los equipos de comunicación se pudo evidenciar como cada paquete que ingresa y sale es marcado con el valor de la clase asignado, como cada una de las listas de control de acceso capturan los paquetes dependiendo de su clase, como se gestionan el encolamiento y la congestión. Los resultados obtenidos cumplen con los objetivos generales y específicos planteados para este proyecto, permitiendo asegurar un nivel de servicio adecuado para cada clase de tráfico dentro de la Unidad de Negocios Termopichincha con la aplicación de un esquema de trabajo que involucraba el análisis, diseño, implementación y pruebas de QoS detallado en el Capitulo 4.
- La aplicación de QoS en los equipos de comunicación wireless fue muy limitado, debido a que el equipo que maneja la comunicación wireless (controladora LAN wireless) posee opciones de QoS que son muy generales y están enfocada a redes dedicadas a manejar un solo tipo de tráfico. En el caso de Termopichincha, las redes wireless manejan tráfico de los 5 tipos de clases. Igualmente en los equipos switch Cisco de capa 2, se tuvo una limitación ya que la aplicación de QoS únicamente se la puede realizar a las colas de salida de las interfaces de acceso. A pesar de estas limitaciones se pudo realizar la aplicación de QoS en el equipo de comunicación más cercano a la fuente del tráfico, respetando la frontera de confianza sobre el marcaje realizado.
- Es importante concluir que la Unidad de Negocio Termopichincha mantiene un control y monitoreo constante de la infraestructura de red y de los accesos hacia las aplicaciones externas (hacia el internet) como internas con el objetivo de brindar un buen servicio a los usuarios, por ello, la implementación de QoS brindará un plus

adicional mejorando el nivel de servicio para cada clase de tráfico dentro de la infraestructura de red.

- En cuanto a los costos, se obtuvieron algunos beneficios a partir de la implementación de QoS dentro de la organización:
    - La disponibilidad de la información hacia las entidades de control, permite la reducción de multas, ahorrando un valor de $5000 dólares al año.
    - El cumplimiento de las medidas de austeridad que atraviesa el sector público, permite el aprovechamiento de todos los medios de comunicación como videoconferencia y telefonía IP entre las distintas centrales de la Unidad de Negocios, eliminado en un 80 % la generación de comisiones de viaje mensual (valor diario de comisión es de $60).
    - Implementación por parte de los proveedores. El ahorro del valor por realizar este tipo de implementación en una organización se encuentra valorada entre los $2000 y $3000 dólares, los cuales varían dependiendo del tiempo de implementación, personal técnico y horas de soporte.
    - Al mejorar la calidad de los servicios internos de la Unidad de Negocios hacia los empleados, permitirá mejorar la producción interna durante el horario de trabajo y por ende reducir costos de horas extras y contratación de personal.
- En cuanto al tema político, debido a que la Unidad de Negocios Termopichincha es una empresa pública que conforma la corporación CELEC EP, está obligada a dar cumplimiento al Acuerdo 003-CG-2015, en la que la Contraloría General del Estado adopta medidas de austeridad con el antecedente del art. 286 de la Constitución de la República, lo que provoca que este proyecto de tesis sea considerado importante para

mejorar los servicios de comunicación como telefonía IP y videoconferencia, brindando mejores servicios a los usuarios y utilizando los recursos tecnológicos de la información que posee la Unidad. Los siguientes puntos muestran los beneficios brindados en el tema de austeridad gracias a la implementación de QoS:

- Reducción en la adquisición de equipamiento y productos relacionados con tecnología de la información y comunicaciones.
- Uso de medios tecnológicos disponibles en la entidad para la reducción de costos por desplazamientos de personal.
- Optimización de la infraestructura de tecnología de la información y comunicaciones que actualmente se encuentra disponible en la entidad.

5.2 Recomendaciones

- Para evitar los problemas de interconexión entre los canales de fibra óptica multimodo y monomodo, se recomienda que se realice una migración en el canal de fibra multimodo por fibra monomodo, permitiendo estandarizar el equipamiento de comunicaciones y obtener mayores beneficios al usar fibra óptica monomodo (velocidad y ancho de anda).
- En el caso de alguna falla de software, hardware, físico o lógico en el canal de fibra óptica entre las Oficinas de Quito y Guangopolo, se recomienda implementar un enlace de datos redundante, sea mediante fibra óptica o mediante radio enlace, y mantener en bodega equipos de comunicación redundantes para realizar maniobras emergentes y evitar la indisponibilidad de los servicios.

- Si se desea tener mayores beneficios en cuanto a la implementación de QoS en las distintas Centrales remotas de la Unidad de Negocios Termopichincha ubicadas en diferentes regiones del país, se recomienda que las configuraciones implementadas de QoS sean extendidas a los enlaces manejados por los proveedores de CNT y Unisolutios (satelitales). Adicionalmente se recomienda habilitar las opciones de QoS dentro del equipo perimetral Checkpoint (Firewall).
- En el caso de los equipos de comunicación, a pesar de que se encuentran en las mejores condiciones y su funcionalidad puede soportar configuraciones adicionales para el beneficio de red, se recomienda que estos sean actualizados a nivel del sistema operativo, tomado en cuenta las mejores prácticas dadas por el fabricante. Adicionalmente se recomienda no descuidar la constante renovación de garantías y soporte técnico en los equipos de comunicación..
- Se recomienda realizar un constante monitoreo de las configuraciones implementadas de QoS en todo el equipamiento de comunicaciones con el objetivo de constatar su continuo funcionamiento. Debido a que los medios utilizados para realizar videoconferencias o telefonía IP son herramientas licenciadas, es posible que a mediano o largo plazo las medidas decretadas por el sector público obliguen a la utilización de software libre, provocando que el tráfico de red generado por otro software sea diferente y se tenga que realizar una restructuración de las configuraciones.
- Debido a que la Unidad de Negocios maneja tráfico de red Administrativa e Industrial en la misma infraestructura, se recomienda que exista una división de la infraestructura de red para que se brinde un tratamiento diferente para la red

administrativa y para la red industrial. La información industrial es considerada crítica ya que las entidades de monitoreo como el CENACE o el MEER regulan y controlan la información en tiempo real.

- Durante los últimos años ha existido mucha restricción a nivel público en cuanto a las Tecnologías de la Información, que provocan que muchos de los proyectos propuestos en mejoramiento continuo no sean ejecutados, debido a ello es recomendado que el área de TIC realice un constante seguimiento de los decretos y acuerdos que enfocan el tema de Tecnología de Información, con el objetivo de plantear de mejor manera los proyectos y el manejo del presupuesto anual dentro de su Plan Operativo Anual. Adicionalmente es recomendado que se realice un análisis más profundo del equipamiento de comunicaciones y servidores que se maneja actualmente, ya que en ciertos casos estos se encuentran subdimensionados o desperdiciados, provocando que no se optimicen adecuadamente los recursos tecnológicos.

BIBLIOGRAFÍA

[1] Ataucuri, D. D. (1 de 12 de 1999). *sisbib.unmsm.edu.pe.* Obtenido de Calidad de Servicio en la Internet: http://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/electronica/Diciembre_1999/Pdf/02_calidad.pdf

[2] Bravo, B. P. (2011). *Diseño e Implementación de Calidad De Servicio (QoS) en la red de transporte de datos del Municipio del Districto Metropolitano de Quito (MDMQ). Proyecto previo a la obtención del título de Ingeniero.* Escuela Politécnica Nacional - Ecuador.

[3] Cavanaugh, M. J. (23 de 12 de 2004). *ciscopress.com*. Obtenido de Cisco QoS Exam Certification Guide: MQC, QPM, and AutoQoS: http://www.ciscopress.com/articles/article.asp?p=358548&seqNum=4

[4] Cisco. (1999). *docwiki.cisco.com*. Obtenido de Cisco - Quality of Service Networking: http://docwiki.cisco.com/wiki/Quality_of_Service_Networking

[5] Cisco. (08 de 04 de 2014). *www.cisco.com.* Obtenido de Enterprise QoS Solution Reference Network Design Guide: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/QoSDesign.html

[6] Cisco. (25 de 08 de 2015). *cisco.com*. Obtenido de: http://www.cisco.com/cisco/web/support/LA/102/1027/1027812_cat3750-qos-config.html

[7] Cisco System. (06 de 2006). *www.cisco.com.* Obtenido de: http://www.cisco.com/c/en/us/td/docs/switches/metro/me3400/software/release/12-2_25_seg_seg1/configuration/guide/3400scg/swqos.html

[8] Cisco Systems. (2007). *slideshare.net.* Obtenido de Caracteristicas y evolución de las redes LAN y WAN con servicios unificados: http://www.slideshare.net/mundocontact/taller-redes-emergentes

[9] Cisco Systems. (2015). *cisco.com.* Obtenido de: http://www.cisco.com/en/US/technologies/tk543/tk879/technologies_qas0900aecd8020a589.pdf

[10] Cisco Systems. (23 de 04 de 2016). www.cisco.com. Obtenido de QoS: NBAR Configuration Guide, Cisco IOS Release 15M&T: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/configuration/15-mt/qos-nbar-15-mt-book.pdf

[11] Ciscoblog.ru. (s.f.). *ciscoblog.ru*. Obtenido de QOS: http://ciscoblog.ru/?ibsa=get_content&id=364

[12] Elastixtech. (19 de 01 de 2016). *elastixtech.com*. Obtenido de QoS-Calidad de Servicio para VoIP:

http://elastixtech.com/qos-calidad-de-servicio-para-voip/

[13] Gerometta, O. (30 de 09 de 2010). *librosnetworking.blogspot.com*. Obtenido de Modelos de implementación de QoS:

http://librosnetworking.blogspot.com/2010/08/modelos-de-implementacion-de-qos.html

[14] Gómez, R. M. (s.f.). *www.ebah.com.br*. Obtenido de QoS EN REDES DE ÁREA LOCAL:

http://www.ebah.com.br/content/ABAAAgjjIAC/qos-en-redes-area-local#

[15] In Depth Tutorials and Information. (s.f.). *what-when-how.com*. Obtenido de QoS Implementation Methods (IP Quality of Service):

http://what-when-how.com/ccnp-ont-exam-certification-guide/qos-implementation-methods-ip-quality-of-service/

[16] Lin, M. (1999). *Cisco.com.* Obtenido de Quality of Service: http://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/quality-of-service-qos/prod_presentation0900aecd80312b59.pdf

[17] Masadelante. (1999 - 2016). *masadelante.com*. Obtenido de Definición de ancho de banda:

https://www.masadelante.com/faqs/ancho-de-banda

[18] Microsoft. (19 de 01 de 2016). *technet.microsoft.com*. Obtenido de Calidad de servicio basada en directiva (QoS):

https://technet.microsoft.com/es-es/library/jj159288.aspx

[19] Oocities. (19 de 01 de 2016). *oocities.org*. Obtenido de Modo de Transferencia Asincrónica (ATM):

http://www.oocities.org/espanol/nivelredes/hardware/foro/ATM_Foro.htm

[20] Oracle Corporation. (2010). *docs.oracle.com.* Obtenido de Guía de administración del sistema servicios IP:

https://docs.oracle.com/cd/E19957-01/820-2981/ipqos-intro-54/index.html

[21] Rahul Kachalia, Cisco Systems. (2010). *Technical Marketing Engineer, Systems Architecture & Strategy.* Obtenido de http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/Borderless_Campus_Network_1-0/Borderless_Campus_1-0_Design_Guide.pdf

[22] What-When-How. (s.f.). *what-when-how.com*. Obtenido de Classification and Marking (Classification, Marking, and NBAR):

http://what-when-how.com/ccnp-ont-exam-certification-guide/classification-and-marking-classification-marking-and-nbar/

[23] Wikipedia. (21 de 12 de 2015). *Wikipedia*. Obtenido de Multiprotocol Label Switching: https://es.wikipedia.org/wiki/Multiprotocol_Label_Switching

[24] Wikipedia. (s.f.). *es.wikipedia.org*. Obtenido de Calidad de servicio: https://es.wikipedia.org/wiki/Calidad_de_servicio#cite_note-itu-t-2-2

[25] Wong, N. (14 de 02 de 2012). *prezi.com*. Obtenido de: https://prezi.com/c1qqzrkr2nwa/qos/

[26] Chafla, F. (2014 - 2015) "Calidad de Servicio QoS en Redes TCP/IP" [Material Didáctico]. Maestría en Redes de Comunicaciones, PUCE

[27] Cisco Systems. (2010). *www.cisco.com*. Catalyst 2960 and 2960-S Switch Software Configuration Guide. Obtenido de: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/qos/command_reference/b_qos_152ex_2960-x_cr/b_qos_152ex_2960-x_cr_chapter_011.html

[28] Frahim, E. Froom, R. Sivasubramanian, B. (13 de 05, 2004). *ciscopress.com*. CCNP Self-Study: Understanding and Implementing Quality of Service in Cisco Multilayer Switched Networks. Obtenido de: http://www.ciscopress.com/articles/article.asp?p=170743&seqNum=7

ANEXOS

ANEXOS 1: PROTOCOLOS QUE CIRCULAN EN LOS DIFERENTES ROUTERS DENTRO DE LA INFRAESTRUCTURA DE RED DE LA UNIDAD DE NEGOCIOS UTILIZANDO EL MECANISMO DE NBAR.

	Protocol	Input	Output
		Packet Count	Packet Count
2	ftp	11073161	22532793
3	http	18065906	14321724
4	cifs	69491996	41831263
5	binary-over-http	32411060	20628865
6	ssl	15485128	10284406
7	notes	7653082	7051497
8	imap	1582651	1817162
9	video-over-http	35505	58675
10	dns	2161800	1561381
11	ms-live-accounts	897163	827781
12	smtp	618780	298975
13	ms-wbt	1176923	1227234
14	rtmp	675629	385987
15	skype	461674	508420
16	rtp	6923396	6876449
17	webthunder	1296001	895540
18	secure-http	138553	144659
19	ms-update	139313	90550
20	ms-office-365	43762	40324
21	share-point	20764	15534
22	gmail	951602	776999
23	flash-video	43396	27656
24	dnp	23507607	26939500
25	pop3	11357	8272
26	secondlife	30808	30848
27	netbios	241373	153118
28	google-accounts	820634	595968
29	virtual-places	363721	348440
30	sqlserver	13710	19690

31	opsmgr	7725	6144
32	kerberos	859660	602643
33	microsoftds	2017	1172
34	exchange	5272	4546
35	ncube-lm	6233	12915
36	activesync	6261	5114
37	asa-appl-proto	16178178	12865399
38	oracle-sqlnet	8784	14717
39	ms-netlogon	106669	133831
40	ms-rpc	168526	213964
41	itunes	5909	4613
42	vnc	4083	3289
43	active-directory	282651	289736
44	gotodevice	3386	2480
45	gsiftp	2670	1963
46	ldap	106029	99238
47	webex-meeting	12031	13472
48	netbios-ns	37108	1079658
49	youtube	894	710
50	mgcp	6544	4578
51	bittorrent	384	364
52	ping	354818	393772
53	snmp	337755	560776
54	esignal	338	192
55	icmp	54210	136873
56	hp-pdl-datastr	154	89
57	telnet	14416	22066
58	encrypted-emule	1863	1997
59	poco	7033	7060
60	rtmpt	84	52
61	sip	397	2861
62	http-alt	164	157
63	h323	3775	3697
64	stun-nat	0	1971
65	nntp	43	67
66	tcpoverdns	206	211
67	audio-over-http	96	88
68	avocent	27	14
69	dnsix	20	21
70	xmpp-client	88	87

71	novadigm	11	11
72	teamsound	7	21
73	rtcp	26444	27093
74	isakmp	492	28
75	dht	0	685
76	winny	73	66
77	oraclenames	34	34
78	aol-protocol	19452	9731
79	socks	17612	8818
80	svrloc	3485	3414
81	teredo-ipv6-tunneled	0	1758
82	secure-imap	535	486
83	sunrpc	0	1084
84	netflix	118	116
85	ntp	0	474
86	teamviewer	46	32
87	rtsp	47	41
88	msn-messenger	4	8
89	ms-sql-m	0	13
90	realmedia	4	2
91	xdtp	4	4
92	micromuse-lm	3	4
93	isatap-ipv6-tunneled	0	1
94	unknown	14506865	19872012
95	Total	229498429	196718407

Datos NBAR router WAN hacia CELEC

		Input	**Output**
	Protocol	Packet Count	Packet Count
1	http	23125099	45478565
2	ssl	23487852	18315633
3	cifs	5133852	74547279
4	binary-over-http	918025	575077
5	notes	8246251	8812203
6	itunes	443717	337239
7	rtcp	125052	351867
8	video-over-http	169882	94847

9	secure-http	356037	331323
10	imap	1952407	1522408
11	ms-wbt	1225010	1645570
12	ms-update	61035	321197
13	smtp	291913	1025706
14	webthunder	1454346	989956
15	skype	1178785	1374347
16	rtp	6928217	6980498
17	ms-live-accounts	941949	822701
18	rtmp	1754390	961002
19	share-point	79036	46194
20	gtalk	71041	80762
21	gmail	339517	267480
22	flash-video	82366	51497
23	google-accounts	918840	704680
24	ms-rpc	2122997	3046300
25	dnp	26227914	22059473
26	rtmpe	3909	2044
27	secondlife	30848	30808
28	netbios	12998	242785
29	virtual-places	382840	401723
30	kerberos	604003	861615
31	opsmgr	6144	7725
32	audio-over-http	3839	2520
33	stun-nat	3018	13991
34	microsoftds	4	2013
35	dns	1797537	2036049
36	asa-appl-proto	12894029	16224163
37	ms-netlogon	134023	106793
38	pop3	2113	1422
39	gsiftp	1963	2670
40	gotodevice	2480	3386
41	ldap	105697	111992
42	ms-office-365	20771	17234
43	active-directory	290915	284647
44	ftp	11	223209
45	webex-meeting	11586	13804
46	oracle-sqlnet	2932	8784
47	mgcp	476	8194
48	tcpoverdns	133514	168320

49	sqlserver	91	13540
50	youtube	471	420
51	secure-imap	3398	2810
52	snmp	32097	564060
53	ping	335718	464109
54	netbios-ns	14202	360309
55	rtmpt	1594	627
56	realmedia	830	768
57	telnet	1284	1676
58	bittorrent	206	148
59	poco	9879	9890
60	icmp	104510	8277
61	sip	30225	30208
62	ncube-lm	70	6153
63	encrypted-emule	1340	1687
64	nntp	119	150
65	h323	4921	5030
66	xmpp-client	319	353
67	citrix	0	123
68	google-earth	61	53
69	socks	41	54
70	rtsp	0	13
71	edonkey-static	0	71
72	netflix	187	187
73	oraclenames	34	34
74	irc	0	5
75	teamviewer	33832	37059
76	aol-protocol	9731	19452
77	ntp	0	3765
78	isatap-ipv6-tunneled	0	595
79	isakmp	180	0
80	dhcp	0	69
81	winny	131	133
82	dht	0	188
83	teredo-ipv6-tunneled	0	116
84	teamsound	0	116
85	http-alt	39	30
86	encrypted-bittorrent	16	0
87	epmap	0	10
88	ms-sql-m	13	0

89	msn-messenger	2	2
90	ipv6inip	0	19
91	xdtp	4	4
92	sip-tls	0	4
93	unknown	17146853	29748091
94	Total	141813637	242800678

Datos NBAR router WAN hacia Guangopolo

		Input	Output
	Protocol	Packet Count	Packet Count
1	http	43237559	22069982
2	secure-http	24695046	29431189
3	microsoftds	61440152	48506
4	cifs	13011288	5092666
5	skype	300045	480261
6	imap	1693145	2039017
7	smtp	596120	282324
8	ftp-data	10737886	0
9	hl7	190949	347276
10	notes	90697	31295
11	fasttrack	2684	8564
12	h323	310638	253826
13	novadigm	16804	10281
14	914c/g	8316	14181
15	edonkey	10556	18426
16	dns	1417970	1223705
17	netbios	902866	49423
18	exchange	929575	1205492
19	kerberos	1123600	1125177
20	asa-appl-proto	599147	512564
21	rtp	11553	9267
22	icmp	1417901	463234
23	pop3	1236	1963
24	ldap	188504	189726
25	secure-imap	76376	77476
26	ftp	224483	79
27	rtcp	3240	2944

28	pcanywhere	1077	1577
29	skinny	8049	2389
30	sap	7558	2058
31	sqlnet	18317	5180
32	mgcp	8221	2753
33	snmp	1364048	832067
34	citrix	5904	1463
35	netshow	2607	566
36	socks	2902	272
37	groove	203	4
38	telnet	3228	2555
39	sqlserver	13954	6
40	aminet	188	6
41	sitaradir	108	4
42	l2tp	141	2
43	sip	8944	8945
44	xwindows	123	24
45	coauthor	23	3
46	streamwork	10	1585
47	stun-nat	1637	28
48	youtube	287	260
49	vnc	89	0
50	cuseeme	30	0
51	pptp	38	4
52	pip	26	6
53	net-assistant	33	6
54	shockwave	54	4
55	sitaramgmt	40	2
56	oraclenames	24	7
57	vdolive	22	0
58	rmiregistry	27	1
59	rtsp	14	0
60	rmiactivation	23	2
61	wap-push-http	17	0
62	nfs	15	0
63	sitaraserver	24	4
64	directv-soft	14	2
65	tlisrv	16	2
66	net8-cman	23	2
67	directplay	21	2

68	wap-push-https	14	0
69	ntp	57830	11222
70	svrloc	329	7
71	wap-push	11	0
72	ms-sql-m	6323	1
73	ipv6inip	614	0
74	dhcp	69	0
75	ms-olap	10	2
76	xfer	20	23
77	rsvp	9	3
78	micromuse-lm	6	2
79	directv-tick	12	2
80	oraclenet8cman	9	0
81	blizwow	7	1
82	gtp-user	9	1
83	ora-srv	9	4
84	kali	7	1
85	xdtp	8	0
86	lockd	6	1
87	rdb-dbs-disp	5	5
88	wap-pushsecure	6	2
89	mysql	7	0
90	contentserver	4	0
91	worldfusion	3	3
92	directv-web	3	0
93	msft-gc-ssl	5	0
94	msnp	2	0
95	orbix-loc-ssl	4	0
96	directv-catlg	2	1
97	sqlexec	5	0
98	msft-gc	2	0
99	orbix-locator	3	0
100	orbix-config	1	2
101	Konspire2b	1	0
102	unknown	79924856	78898699
103	Total	244676733	144760619

Datos NBAR router WAN hacia Quito